TICOM/I-206

U-4 2-2

14-2

EXTRACTS FROM HOMEWORK WRITTEN BY MIN. RAT WILHELM FENNER OF OKW/CHI.

Attached is a selected translation of the written homework of Wilhelm FENNER, Ministerialrat of the Signals Intelligence Agency of the High Command, German Armed Forces (OKW/Chi), which has been prepared by A.S.A. Washington.

2. Due to the length of the paper written by FENNER for TICOM, this translation is only a summary. Inquiries concerning the detailed German original should be addressed to Ticom.

TICOM
7th August, 1947.

No. of Pages : 40

Copy No : 22.

Distribution :-

L.S.I.C.

1. T
2. S
3. H
4. M
5. L
6. Z
7. H.71
8. H.62
9. H.63
10. L.91
11-14. Ticom Files.

U.S.

15. U.S.L.O. }
16-19. Op-20-2 } via U.S.L.O.
20-23. A.S.A. Washington. }
24. Director, A.S.A. Europe)

External.

25. Signals 6, War Office.

Do NOT Destroy Return to the NSA Technical Library when no longer needed
S-4899

~~TOP SECRET~~

F

1. The attached is a selected translation of the written homework of Wilhelm FENNER, Ministerialrat of the Signal Intelligence Agency of the High Command, German Armed Forces (OKW/Chi).

2. Due to the length of the paper written by FENNER for TICOM this translation is only a summary. Persons interested for expansion upon any point should address inquiries to TICOM where the German original is available.

3. In general FENNER is believed to have presented an accurate and complete picture of the history and operations of OKW/Chi within the limits of his memory. The homework is chiefly of value for the history of OKW/Chi (or its predecessors in the German Reichskriegsministerium and Reichwehrministerium) from 1920 to VE day. The information available from this source considerably expands and to some extent modifies the history of the Signal Intelligence Agency of the High Command German Armed Forces and of the Signal Intelligence Agency of the German Army High Command given in Volume III and IV respectively of European Axis Signal Intelligence in World War II As Revealed By Ticom Investigations And By Other Prisoner Of War Interrogations And Captured Material, Principally German, ix vols. WDGAS 14, 1 May 1946.

Translated R.W.P.
WDGAS-14
26 May 1947

RECORD COPY
DO NOT DESTROY OR MUTILATE

NSA LIBRARY
S-5454
FAV

~~TOP SECRET~~

S-5454

This report comprises a total of 244 pages in three volumes. Save for two questions which he misunderstood, the answers are considered honest and and as full as he could be expected to give. A list of topics is appended, where no mention is made in the following, it is to be assumed that his answers contained no information of importance, or were purely negative.

Volume I gives a description of OKW/Chi as of 1939 and 1944 with a few notes regarding changes in competence at the end; a description of Mr. Fenner's cryptanalytic career from 1921 on and finally a record of successes achieved by OKW/Chi from 1938, on listed by countries.

Volumes II and III contain answers to specific questions. Such as appear of any value are either translated in full or summarized in the order in which they appear in the full list.

A few terms:
Angestellter (fem. Agestellte) is a civil employees, not appointed for life and with no pesion rights, not military.

Wehrmachtbeamter is not an officer and has no power to impose disciplinary penalties. Appointed for life and has pension rights. In contrast to the Angestellter he is subject to military penal law (wears uniform in wartime) but may choose his own political party.

Ein beorderter Beamte is one released by a non military agency for service with the armed forces.

Parallelstellen (parallel passages) sometimes signifies "repeats" but frequently we might say "isomorphs". Perhaps the latter meaning is more frequent in this paper. (i.1)

Page references to the portion summarized will be indicated in parentheses as above.

Volume I.
1. OKW/Chi. The information is rather complete considering the fact that Mr. Fenner had to rely on memory. It can be used to check the Report of the Tiemm Committee (i. 1-13)

Observations:

Speed was all important.

Collaboration was generally good with the Hungarian, Finnish and Italian cipher outfits and with the Foreign Office, there was no such relation with Goering's Forschungsamt. The foreign groups supplied intercepts and solved groups, most of the traffic exchanged was sent by courier, in rare cases Hungary sent by telegraph. Copies of land line and cable messages were obtained from the Forschungsamt through the Foreign Office, an unsatisfactory arrangment. OKW/Chi controlled two fixed intercept stations for wireless traffic.

The logging section (Hauptgruppe B) often handled over 1000 messages in a day; it prepared the duplicates for foreign units, sifted out worthless material which was not counted, in fact no mere "statistics" were prepared for show.

Translations were as factual and close as possible, any doubtful passages were clearly designated as such.

Security regulations were enforced; daily inspection was made of each room to see that everything had been properly locked up. Only male personnel had keys to safes.

To January 1933 monthly reports on progress were expected and these were quite full, then after Hitler came into power and the Forschungsamt was established, mistrust of the latter led to a reduction of reports to an annual, uninformative basis. (i. 13-16)

Mechanical aids were developed to speed the work. These included:

a. Roellchengeraet. A device with 10 x 10 wheels, wach with the digits 0 to 9 inscribed at equal intervals around its edge. The device, front view, measured some 20 x 30 cm. It was used to compute difference where a fairly long additive sequence was used. Mr. Fenner never used one but several were used in his section and were considered satisfactory. Developed by the Foreign Office.

b. Electric typewriter. Used to convert code enciphered with a simple substitution table (such as Romanian messages). By 10 switches and 10 relays the numeral keys of one machine were connected to the numeral bars of another, the substituted digits were printed under the cipher groups of the message. The improved model had ten special keys for the digits wired to the regular digit keys; the operator typed the cipher text and printed the plaintext (i.e. solved the substitution) in groups of five digits, beneath the cipher. It worked well but of course the key had to be recovered before one could use the machine.

c. Das grosse Differenzenrechengeraet. This was a typewriter combined with punch tape reader and relays. It was used to get automatically the differences of all the groups in a message. The cipher text was punched on tape, two congruent tapes were run through the reader so that position 1 of tape I was matched successively with positions 1, 2, 3,.....n of tape II, each resulting difference was determined and automatically typed. Then position 2 of tape I was compared with all positions of tape II, &c. The device was used on Polish ciphers and ran for hours at a time at a speed of about 5 characters a second; line advance and space between groups was automatic. Developed and build by Chi H Gr B.

d. Bigramgeraet. Had 262 relays corresponding to the normally possible bigrams. Looked like an upright metal frame some 200 cm high and 100 cm wide to hold relays. Messages had to be punched on tape, then all positions of I were matched with all positions of II. As Mr. Fenner recalls, the result was scanned and recorded graphically on a tape. If at a given position of the two tapes one found the frequencies of normally expected bigrams, then that was a "weak point" of the system. In contrast to the Differenzengeraet this device scanned a series of punch positions, which series was predetermined. It was used with success on Japanese systems but was too sensitive for continuous use. Developed and built by Chi H Gr B.

e. The Phasensuchgeraet. If it was suspected that a phase was repeated in a cipher text this device was used to find this phase L automatically. The text was punched, scanned and recorded graphically on a paper tape some 30 cm side in the form of small strokes. The tape was now advanced one position and scanned again (ll-paralell in respect to the first graphic record) and where like punched sequences occurred a visially thicker (denser) series of symbols resulted. If finally phase L lay beside L_2, then on the basis of p probability visually obvious peaks must result on the paper strip which would be higher than were phases L_1, L_2....L_n did not lie side by side (?). A like interval between peaks was phase L assuming that L_1, L_2, L_3.....= L_n. The device was practically never used. It was developed and built experimentally by H Gr B.

f. Hollerith machines. When there were great masses of Polish ciphers to work these were sent to the unit "Maschinelle Berichterstattung" with a request that differences be computed. The machines worked well but it is certain that for certain purposes smaller, speedier machines using less material would be more to the point. The whole problem of auxiliary machines tended toward optical scanning since mechanical devices were too slow.

g. German cipher machines. Development was in the hands of the Waffenamt. Chi was, to be sure, concerned with criticism and analysis but only gave suggestions, it could not construct any. The Enigma was considered outmoded although secure when correctly used. The Geheimschreiber (G-schreiber) was modern but not mobile enough. All plans for new developments were doomed by the end of 1944. No more practical work could be undertaken. (i. 24-48)

Organization of Chi in 1939 (just before the war).

The war brought no change in organization. In 1938 (?) there was a discussion of needs in case of mobilization but this merely provided for an addition of about 30% to personnel; no one knew who might be at war, so no one could foresee needs.

With the outbreak of the war Chi (still called Chiffrierstelle in 1939) became a part of Inspektion der Nachrichtentruppen and had four Gruppen, each with several Referaten.

Comparison 1939 and 1944: No essential change. One important point is that in 1944 the development of all cryptographic systems for the army was turned over to Chi. Purpose was to concentrate all cryptography of the armed forces in one unit, including the SS, actually every branch of the service went its own way, rarely asking Chi's approval. An order to this effect was issued in 43 but even in early 44 little heed was given it. One defect, in Fenner's view, is that the oversight was not given H Gr B, where there were trained people, but to a new group.

Otherwise there was a great increase in personnel over 39; analytic machines had been developed; the amount of traffic had swollen immensely; collaboration with Rome was added, but due to mistrust on both sides was never very fruitful, it was broken off after the Allies invaded Italy. (i. 29-40)

Fenner's LIFE with which the development of Chi is sketched. (i. 40-57)

Chi's successes from 1938 on. (By countries)

Mr. Fenner says his memory would not permit giving much of an account of purely analytic successes, hence he has not limited himself strictly to those.

1. Russia. The system OK and its successors were worked on and solved from the first appearance down to the summer of 1943. Mr. Fenner thinks the first was OK5, OK6 and OK7 were surely solved, and - he believes - also OK8. He thinks they were 4 digit codes with partial encipherment by 2 digit substitution tables. After a few were captured solution became easier since the entire vocabulary was known, Helsingfors worked successfully on the solutions and was sometimes faster than Chi. Work was also done on the NKVD cipher but Mr. Fenner never saw any tangible results. His men who had been taken by the Air Force came back in the summer of 1943 and after that he never heard whether either army of airforce had any success. Often it was so reported but he did not see any positive results. If solutions of code with virtually endless additive sequences were achieved, it must have been where, by error, the additive was used more than once, otherwise solution would have been impossible. It was clear that when additive blocks were captured they could not be used let alone had any right to be used unless in case of some catastrophe where no other means of encipherment was available.

Not worked on were the ciphers Polpred and Narkomindel, also other diplomatic ciphers, because of the endless additive sequences were surely not

~~TOP SECRET~~

repeated, hence no method of reduction could have been found. Furthermore it was to be assumed that the basic code had groups of different lengths. (i. 66-67)

2. Poland. Since its introduction of additive sequences for encipherment of its diplomatic 4 digit code Poland had repeatedly improved its systems during the years. The sequences were 40 digits long, later basically a multiple of 4 plu 1 or plus 3. E.g.: L= 50 x 4 plus 1= 201. Solution of such additives depended entirely on the amount of material at hand. But whereas at the outset an endless additive sequence (as Mr. Fenner recalls it) was used for a fortnight, certainly was used more than once (and there were encoders who habitually started at the same point), later the sequences were replaced more often and were different for each circuit, e.g. Warsaw-Berlin, Warsaw-Washington; indeed, at the end,ie. just before the war began, the endless sequences for Warsaw-Berlin were different from those for Berlin-Warsaw. And changes came so fast that even with more fully solved codes messages could no longer be read because no two messages were ever found in the same key any longer. Most of the later messages of the Exile Government in London and the Resistance Movement were solved. The differences were calculated mechanically. Mr. Fenner cannot describe another complicated system, he ventures, with caution, the opionion that substitution tables were used for encipherment, these appeared unsystemmatic but were actually systemmatically laid out according to certain laws of the theory of groups. The basic system was probably a so called 2 digit digit Caesar (2 digit substitution). Mr. Fenner assumes it is known that the Poles had an excellent connection with the Fuehrerhauptquartier and got excellent strategic information promptly. The indicator for this agent was a 3 digit number (406??). In any case the heads of OKW and of the German Government knew from decrypts of Polish demands for the cession of Pommerania, which they claimed as having once belonged to Poland, and also of the disappointments occasioned repeatedly by the Russians after the German front was driven back. (i. 66-68)

3. Czechoslovakia. No traffic after 1939. Up to then not a single system had been solved. Apparently a letter subsitution was used but the type of encipherment was not discovered. No repeats were found. During the war Czech ciphers were found sporadically, but all with keys. As far as Mr. Fenner recalls they were 2 digit substitutions, the contents related to connections of confidential agents. (i. 68)

4. Yugoslavia. Systems of the Government in Exile were those used in peace time and were read currently, with interruptions whenever a code or encipherment was changed. The systems was a 5 letter code and a digraphic substitution table. They always facilitated solution of government traffic; either the new code was merely a systemmatic shuffling of the old one, e.g. by shifting page numbers, or when a really new code was introduced the old tables were kept in use. All that was needed was adequate traffic volume, even when the encipherment changed daily. The numerous variations used were not adequate to insure security. It was a fine example of a system which lowered its limit of resistance by poor use. If Yugoslavia had once introduced a completely new code and simultaneously a new table, say about 1940, not a message would have been read, due to the scant material. The last variations were complicated; instead of enciphering two adjacent ~~dl~~ letters, vertical pairs were taken; e.g. no longer 12 45 67 80 92 23 45 46 71 45
ka ro sa tu pi la ro bi mi ro

but

~~1 2 4 5 6 7 8 0 9 2~~
~~2 3 4 5 7 8 0 1 6~~
1 2 4 5 6 7 8 0 9 2
2 3 4 5 7 8 0 1 6 0
kalafisisa.....

~~TOP SECRET~~

with numerous variations in the manner of forming the pairs. Even though solutions was facilitated by the above mentioned factors it was not easy because of the pairing of heterogenous letter groups. At least 500 10 letter groups were needed to reduce with certainty. Hence toward the end many messages remained unsolved. The content of the messages was always factual and of importance. (i. 68-70)

5. Romania. Used for 20 years in most stereotype fashion a 5 digit code with digit for digit substitution tables, e.g. 0-4, 1-1, 2-6, 3-0, ...
The though that there are 10!-1 different tables possible seems to have led Bucarest to think the system secure. Although solution was not very difficult, since despite all encipherments all affinities remain (e.g. 13316=24429 =90096) (isomorph) and reduction to basic code was possible with enough traffic, Bucarest facilitated solution by using old and new code side by side because remote legations had not yet received the new code, and so an old and a new code were enciphered with the same tables. Sometimes with a new code the new table was forgotten, or the same message was enciphered with old and new code. No other country ever compromised its own systems with such fatal regularity. In 43/44 a new code (5 digit with endless additive sequence) was introduced. However, there was this error: The additive sequence (well over 5000 digits long) was allowed to be reused because it was not possible to supply remote legations with enough cipher material. Now it was worth while to obtain differences although the difference catalog contained several hundred thousand groups. It was done mechanically. It proved useless, however, because the Romanian government collapsed, followed shortly by the German. The value of the Romanian traffic varied greatly, according to the embassy involved.

More interesting was the system of the military attache, a system of coupled transpositions (Wuerfel), the Wuerfel (matrices) changed daily and the plaintext was inscribed in a definite manner. These messages contained very valuable information, e.g. the rapid breakdown of the Romanian army due to poor supply of ammunition, arms and rations. (i. 70-71)

6. France. The peak of successes was from the last of the peace period to the capitulation of France. No other European state used so many systems, Often over a dozen in use at one time. Systems which could not otherwise be recognized at sight carried an indicator at some specific position in the cipher text. This applied to the majority of plain 4 digit codes, each with a series of indicators. These were recognized without great difficulty and combined into tables. Because of structure and paucity of the diplomatic language solution was rather easy, in any case not comparable to the extensive American or British codes or the grammatically difficult Polish codes. The French used these unenciphered codes freely even for important material, enciphered code was less used. As long as 2 digit substitution tables were used for partial encipherment, solution was achieved regularly if enough traffic was received. The unchanged portions of the otherwise enciphered groups gave an important criterium. I have in mind the system with many variants, e.g.

0123 4567 8911 4609 ....

where the tied digits were enciphered by 2 digit tables, the digits marked with x remained unchanged, i.e. were elements of the basic code. However, when during the war the French enciphered all pairs in turn, solution failed; nothing positive could be won from the relativities although at first glance the system appeared even simpler:

TOP SECRET

At the moment I do not recall other encipherments.

When after capitulation France was requested to deposit certain codes (code depose) the French made almost no use of these. France was allowed free use of its Colonial cipher (not solved by Chi) and apparently the most important traffic was sent in this system. Attempts to solve it were unsuccessful. Moreover de Gaulles' cipher was never solved.

Before fighting began the military cipher of higher echelons had been solved, a 4 or 5 digit code systemmatically transposed (tableau carre), i.e. a 2 digit transposition matrix. Some short repeats were found in the cipher text, the interval was constant and could only correspond to the width of the box. If I am not mistaken the keys for derivation of the box were taken from the English code book. Despite all the clever points of this system the appearance of short repeats was its undoing. The decrypts permitted following the French army even far back from the front. (i. 72-74)

7. Belgium. Used a 5 (?) letter code with a substitution table associated with the date. It was solved so long as enough traffic came in but Mr. Fenner no longer recalls details. After the capitulation of Belgium few messages were intercepted so that this source had little value. (i. 74)

8. Netherlands. Had a French code with encipherment but Mr. Fenner no longer recalls any details. In about 20 years only two Belgian (sic!) diplomatic ciphers were solved. (i. 74)

9. Switzerland. Had French and German codebooks, also a machine cipher (Enigma). The two codes were solved. Mr. Fenner thinks several substitution tables existed which might be used simultaneously, each enciphering sections of text of equal length. He thinks certain pairs of digits were replaced by a single digit. No very great results. (i. 74)

10. Egypt. A plain French code was met rather rarely, it was solved. (i. 74)

11. Italy. For years Italy used a 5 digit code with 2 letter substution table. Mistakes were made constantly. In these codes the values are not distributed over the whole range of 10^5 groups but whole hundred blocks were left blank, i.e. never occur. This was important in solving the encipherment because "impossible pairs" could be eliminated. Tables once used, were not only reused after some years but were reused according to calendar so that when a solved table was at hand, it was only necessary to decipher;

If a new 5 digit code was introduced one did not take care to use new tables on all circuits so that the new code was soon compromised. This continued on into the war till Italy, already out on a limb in a military way, introduced the socalled Littoria type with Impero type encipherment which Chi did not succeed in solving. The chief reason for failure was the sharp decline in traffic. Mr. Fenner cannot give details of encipherment but thinks additive (Zahlenwurm) was used. Italy did use the groups of its own outmoded codes for recipherment additive. (i. 75)

12. England. In the course of years some 25 different systems were observed and some 10 plain codes (non-alphabetic, unsystemmatic 5 letter codes) of considerable size were solved. Solution depended solely on the amount of material. The Prodrome messages, assumed to be enciphered with an endless

messa[illegible] appear to have been sent in from Rome there was relatively [illegible] value [illegible] decrypts. When, before the Allied landing, London imposed a traffic blockade there ensued a noticeable decline in the traffic to and from London. But even from the messages of the other European diplomatic agencies not a clue could be gathered as to time and place of the projected landing. (i. 75-76)

13. USA. Brown and Gray codes were solved. Solution depended solely on amount of material, which at times ran very high. Both were held in the original in 1940 (/). Solution of systems designated A5BC9 and A5BC 10 caused considerable trouble. For encipherment of the one 35 (?) strips were used, each with a different substitution alphabet, originally valid in sequence for a rather long time, later (1944?) shifted so often that solution was no longer possible. Fenner thinks he recalls that the number of strips was also increased materially. The original break was not by analysis but on the basis of a codebook supplied by Rome (?) and of tables supplied by Budapest (?). Down to the battles around Tobruk the reports of the military observer in Cairo were probably of great use to Rommel since the American reports regularly gave movements of English troops. The replacement of the system was ostensibly due to remarks in Rome about the breaking of the system, at least some word of this leaked through to German officers in Rome who had not the slightest authorization to know. That solution later was impossible due to the fact that, mathematically expressed, an equation modulo 26 had to be solved each time.

The other system, Fenner thinks, consisted in replacing a limited number of successive letters of the Ztes (=??) by a substitution alphabet according to a table. However, he admits he may be wholly wrong about details, as well as to which system was used by Cairo. (i. 76-77)

14. Denmark. Had a plain (letter ?) code, easily solved but the content made it seem useless to bother with it. (i. 77-78)

15. Norway. Not worked on till after the occupation, then with no results. Hardly 200 messages intercepted in some 4 years. (i.-78)

16. Sweden. The extensive 5 digit code caused much difficulty; after a copy was received from Rome (1940?) it became clear that the philological structure was responsible: Swedish, German, French and English concepts all in one code. This not only rendered all statistics so useless that for a long time it was thought there must be some analytically unbreakable encipherment, but also made the linguistic solution very hard. Months were spent working in an utterly wrong direction; the mixture of tongues was as confusing as the group appearing in English codes after World War I "repeat the nth group" which might have thousands of meanings. Thus this Swedish 5 digit code was a typical example of a cleverly constructed codebook. The content of the few intercepted messages was usually unimportant.

The majority of the Swedish messages were enciphered on the Hagelin Teknik. However the basket of this device (i.e. the drum with 25 (?) bars and various riders) was probably changed from message to message so that with a practically infinite period of the system even its course (Ablauf) was not to be ascertained. This problem was to become the central point in analysis, all the more since there were rumors that the USA was starting to use Hagelin machines (1934/44) (?)." (i.-78-79)

17. Spain, Portugal, Latin America. Work on Spanish diplomatic cipher

~~TOP SECRET~~

Mr. [redacted] cannot say anything definite about the cipher.

Portugese original code was held, Fenner does not recall whether it was enciphered or not. Traffic was scarce and decryptions sketchy.

The Brazilian cipher was completely solved and an original at hand. Fenner thinks it was a 5 (letter?) code with some primitive cipher.

Primitive ciphers of San domingo, Ecuador and Chile were solved but were of no importance. (i. 79)

18. Hungary. "orked on spasmodically, then nothing for years, the system was known in essence: a digit code with numberous digit substitution tables which were used in constantly changing order and with "jumps" of varying lengths. It was never possible to delimit the length of the individual "jumps" (Spruengen) and eliminate "homogenous" material. (i. 79-80)

19. Turkey. The 5 digit codes were originally enciphered with primitive substiution tables. The codes introduced later (from 1937 ? on) were systemmatically related to their predecessors. At first codes or related system were changed monthly, later short (20 digit?) additives were used which caused no difficulty. Turkey always made the mistake of using known encipherments with new codes. All diplomatic ciphers, save that of the ministery of the Interior, were solved. They yielded valuable information. To March 1945 some 8 codes were solved. England knew the Turkish ciphers were poor and tried to force British ciphers on the Turks but the latter declined to accept. (i. 80)

20. Iran. Only a few primitive systems. (i. 80)

21. Greece. Sent few messages. As far as Mr. Fenner recalls, 3 codes were used, distinguished by an indicator in the third position of one of the early groups, e.g. code . He does not know whether any was enciphered. (i. 80)

22. Vatican. Certainly two systems. One was a plain code, solved. Only unimportant administrative matters, little used. Some sporadic work on the enciphered code but laid aside for want of material to diagnose correctly. (i. 80-81)

23. Bulgaria. Used essentially a 5 digit code with transposition of (or within) the groups. Hence in decoding the groups had to be read out according to a varying "scheme", e.g. instead of 12345 45312. Down to the collapse some 5 such codes were solved currently. Bulgaria made the mistake that a new code really corresponded to its predecessor merely the text digits were subjected to a certain conditionally systemmatic change, so that for instance

from old	arose new
28 456	395 56
28 556	396 56

Fenner thinks that once the line numbers were changed by a similar process. The messages were often informative. (i. 81)

24. Japan. Work began during the war. In spite of the many systems met only some 4 plain codes were solved, the difficulty was largely due to the somewhat ambiguous transcription of Japanese into Latin letters. An interrupted grille, the upper lines with gaps, made more trouble. We had no experience in this field, did not even know the structure of the messages and language.

In working on this cipher the Digram device previously mentioned was

gr... been discovered, the rest of the solution usually w...t alc... with-out ... difficulty. No other country had so many inquiries regard... its own ...ic! Some 12 systems were observed but Mr. Fenner thinks not all rel... material had been recognized and reduced to losest terms. Reports usually of little account. (i. 81-82)

25. China. First observed during the war, had some 10 systems of which three were primitive systems which were solved. Reports of no value. (i. 82)

26. Agents. In the middle of 1944 Fenner took over from the army the work on numerous agents' systems of France, Poland, the Balkans and Italy. Most of these, in all some 60 were known, were based on books or keywords. Double transpositions, transposed substitutions and even substitutions with additive were employed. Fenner recalls only one case (Polish) of solution before the agent was caught. Location of the nets had no significance for decipherment; most ofthe nets were found, the number rose into the hundreds by the end of the war. In 99% of the cases decipherment came too late, i.e. after capture of the agent and the securing of the key-(too late that is) unless the net continued to function despite the capture of the agent. Since Fenner had nothing to do with the agents and never saw them the SD (Secherheitsdients) and Abwehr did as they pleased. Their idea, with which Fenner did not agree, was to step in and arrest, and usually that was the end of the net; he would have liked to watch it, especially if able to read the traffic. Without having exact data on the success of such arrests, Mr. Fenner still believes the agents' systems fulfilled their purpose well and that the service was admirably organized. (i. 82-83)

27. Actual cryptanalysis did achieve good results repeatedly (e.g. Polish systems, Romanian additive, Japanese grille) but never attained its full potential accomplishment. It, more than mere decrypting, calls for undisturbed surroundings (bombing attacks, broken furniture, dirt, cold and chronic undernourishment). Since cryptology in the face of the notably higher standards of cryptography in foreign countries had become a science, it must also be expected that the fruits of cryptanalysis could ripen only slowly. The war period with its growing dearth of personnel and material and the taxing of the individual's strength to the breaking point was not favorable for such development. (i. 83-84)

During the war OKW/Chi watched the cipher telegrams of some 30 countries. When at its best (up to the capitulation of France) as many as 3000 messages were issued in a month. Usually about three times as many were deciphered but not translated. Over a period of five years Fenner's outfit received approximately 370 000 cipher messages a year on the average. The peak for personnel, including clerks, was 250 (1942), from then on it sank constantly partly because of inductions and calls to field service, partly because the head of the Labor Office in Berlin refused to supply the help Chi asked for. At the time of the surrender he had perhaps 120 persons.

Three criticisms of the heads of OKW might be made:
1. The results of decipherment were not properly utilized either because not correctly evaluated or because, assuming correct evaluation, through failure to take the necessary steps.

2. D[illegible] [illegible]ement of economic and commercial messag[illegible] [illegible]s ru[illegible] out [illegible] necessary.
3. C[illegible] was not moved in season to adequate, sage quarters when bomb[illegible] began.

Mr. Fenner thinks these three faults were due directly to the fateful doctrine of Blitzkrieg and to the uncritical belief in a miracle. "However, God can not be bribed and therefore is always on the side of the strongest batallions." (i. 84-85)

Volume II.

Volumes II and III contain answers to more or less specific questions. In some cases the answers are negative, in others they add nothing to what is already known to ASA. # indicates the questions answered.

#1. There was no "Cipher Bureau" in the first World War, work was done at Grand Headquarters and at some army headqurators. The Bureau of the Reichswehrministerium was founded in 1921, 1st Lt. Buschenhagen was the guiding spirit, he had two assistants, Hellmut Mueller and Nikolai Rohen. Other untrained personnel was added. Buschenhagen succeeded in resuing during one of the communist brawls about 100 reports from the old military organization giving accounts of systems in use during the war; these Fenner studied and put in order after he joined the organization. This material was taken to Jueterbog Artillery barracks and either destroyed or taken by the Russians.

The Reichswehrministerium was renamed Reichakriegsministerium after the introduction of universal liability for military service, date of change can be found in various publications, including the "Gesetzsammlung". The change of name meant no change in policy or organization. (i. 1-3)

#2. Liaison with other cryptographic agencies. (already discussed in Vol. I, hence only supplementary information here).

1. Hungary. Interesting to note that Chi tried to make some agreement with the Ballhausplatz (Austrian Bureau) early in the 20's but Dr. Klob refused to collaborate. The Austrians had personal contacts with the Hungarians, the latter learned of the matter and sent two men to Berlin (Col. Wilhelm Kabina and Col Pokorny) where within a few minutes the "Berlin Vertrag" was worked out. It provided for mutual aid in work on Italian ciphers: exchange of traffic, solved groups and special remarks. It was stipulated that no such arrangement be made by either party with a third party without previous notice to the other. This agreement remained in effect over 20 years and terms were loyally observed. Later, as the value of the exchange was realized, exchanges were extended till at the end nearly everything was covered. The Hungarians were less energetic and solved less material but they did contribute many missing messages and other aids.

Heads of the Hungarian Chi were:

Col., later Gen. Wilhelm Kabina (to mid 30's) then for a few months
Feldmarschalleutnant a.D. Wilhelm(?) Pokorny
Col., later Gen. Istvan von Petrikovits (till the collapse). several others are mentioned by name. (i. 3-6)

2. Finland. The new Finnish army owed its best to the men who served against Russia in the Royal Prussian Jaegerbataillon 27 during World War I. This relation led to a sounding out by Helsinki in 1927 of possibilities of collaboration with Chi. When Fenner went to Helsinki in June 1927 the Finns really had no organization but 3 years later Finland was an equal partner in the work. Cooperation was chiefly against Russia. Cooperation continued

TOP SECRET

cau ..ly even after Hitler forbade aid to Finland during t inter War. The ..nish contribution was exact clever decipherment rather .an exchange of intercepts. Col. Hallamaa was the sole head. Dr. Pahle (Palle?) was chief analist, there was a Lt. Miek. oja and in 1927 a Dr. Nieminen was Russian expert. Supposedly a woman had charge of theoretical and practical decipherment during the final years. Schulz might give further details on the organization. (i. 6-8)

3. Italy. When the chief of the Cipher section of the General Staff, Brigadier Gen. Vittorio Gamba appeared in Berlin in the summer of 1938 every one at Chi was surprised; they had heard that the Italians had some sort of organization but did not dream Italy would approach Berlin without invitation. Gamba's two day visit led to an arrangment to collaborate on French material, Rome was able to get along very well with Yugoslav systems. It leaked out that the two navies had been working together for some time which induced the general to sound out Chi. Intercepts and code groups were exchanged by courrier, the only obstacle to a fruitful exchange was that Italy had little and did not stick very well to its contract. Matter sent Baron Fiorio laid around for a long time, questions went unanswered, Italy sent back groups which Chi had sent there some time before. There was plenty of dissatisfaction higher up too but the arrangment was allowed to stand. Fenner with Trappe was sent to Rome to organize matters, Gen. Gamba was most correct but during the entire stay of nearly a fortnight Fenner never saw any table of organization or other data which would give him any insight into the size and workings of the bureau. Only the navy had adequate intercept facilities, Italy did not have enough people who could really read and write to man stations. However, they were good bargainers or thieves. they had some codes complete. Italy read some plain French codes, plain English and American, and strangely enough an enciphered Yugoslav system which called for a lot of patient work to break and had bothered Chi in Berlin. Rome also had a Turkish code which Berlin was trying hard to break. Rome finally found the exchange so valuable that it began to do a bit better. Its weakest points were France and its own systems! Rome insisted on aid against French systems, Berlin insisted on improvement of Italian codes, the risk of important leaks was too great. Fenner does not think Rome was actually trying to block, just was unable to do anything satisfactory due to want of competent personnel. Also there was not the same open honesty as was found with the Hungarians and Finns. Then some of the men in Italy began to complain that Gamba was too old. When Italy's collapse became a certainty the collaboration was let drop and requests by the North Italian Fascist outfit for further collaboration, met a deaf ear. Any further cooperation was left up to the navy. (i. 8-13)

4. Japan. Col. Hayashi, chief of the Japanese Cryptographic section and later military attache in Berlin, tried to work at Chi. He brought the American Brown and Gray codes and seemed ready to collaborate freely but he had no decent connection with his own government and so could do little. There was no East Asia Russian traffic he might work on so that his supposed knowledge of a system used in Manchuria could not be checked. He was a welcome guest and general matters were discussed with him but that was all. The general instructions till summer of 1944 were to go easy with Japan, then for some reason not known to Fenner Hitler ordered that all secret matters be revealed to the Japanese. (I. 13-15) General Headquarters had scruples about letting Hayashi have too much, he was given selected "decodes (VNs) from time to time.

TOP SECRET

Des[illegible]od will on both parts, conditions were not favorable for a[illegible]rue coll[illegible]tion. (i. 13-15)

Croatia. This new state had visions of a cryptologic unit; enthusiasti[illegible]unger officers argued for a cipher section, older men saw the other side: lack of resources. No intercept service, hence no fruitful work possible. (i. 15-16)

6. Bulgaria. In autumn 1943 a commission of officers and subalterns appeared in Berlin requesting training. Bulgaria had repeatedly made such requests before and sent a staff officer Michailoff to Chi for help on a Romanian cipher. The cipher was explained but later inquiries showed that the explanation was not comprehended. The 1943 mission appeared more hopeful but was not welcome, however, since it had been approved, they were given a course in general principles with special attention to Yugoslav systems. The officers evidently realized that without an intercept service they could get nowhere and no further requests came from Sofia. (i. 16-17)

7. Romania. No reports of a cipher bureau like Chi in Bucarest. Their own ciphers were so bad one could hardly assume any such bureau. Mr. Fenner assumes the OKH Chi was forced to take action for improvment of Romanian military ciphers. (ii-17)

8. Spain. German volunteer cryptologists worked in Spain during the civil war but they were not under Fenner's control nor did they make any reports to his outfit. Work was chiefly on Red traffic and most of it was solved. Chiefly primitive transpositions and substitutions. Once the Legion Condor asked RKM Chi to solve a Red system. Later inquiries regarding French plain codes came in, usually about indicators or whether Berlin was reading a certain type. Whenever Fenner asked the source of such inquiries he was told: Sarmiento, supposedly an officer who was courteous and of high ideals. Fenner was never in Spain and knew no Spaniards, merely assumes from the inquiries that there was some organization. (ii -18)

9. Concluding remarks. Fenner can venture no estimate of the influence of other groups on foreign units but in the realm of cryptology he is sure that Chi was the important center whose judgment was considered final and correct. Attempts of some foreign agencies to bypass Berlin always ended in failure. Chi learned that Petrikovitz went to Helsingfors, Brcic to Rome, Seifert (during the Schuschnigg tension) to Budapest but said nothing. Berlin's central geographic position and communications lines meant much but also the precision, diligence and speed of Chi's workers made for leadership.

During the mid 30's connections existed with the Estonians but Fenner knows no details of arrangments save that two officers OUN and KALMUS worked for a time in the Russian section, as he recalls it on a small code of some 1000 groups, part of the digits were enciphered. Code groups, encipherment details and observations but not traffic entered into the exchange with Reval. Oun was said to have escaped to Finland when the Russians came in. (ii 18-19)

Collaboration with other German units.

1. Navy. "M" (short for the official OKM/4 SKL III) was older (from before World War I) than OKW/Chi and housed nearby in Berlin. Worked almost exclusively on foreign naval traffic plus the british plain codes employed for communication with the colonies. There was no room for jealousy or occasion for friction. Reports were interchanged but the fields were so different that these were rarely of much help; when any one though he had a helpful idea he went direct to some one in the other outfit with it. Intercepts belonging to other outfit were passed on promptly. Chiefs of M known to Fenner were:

Kapitaenleutnant Rieperzky (shortly after World War I), Kapitaenleutnant Mossel, and shortly before the last war a Kapitaen R.... (name forgotten). Fenner also knew Tranow and Franke (at last accounts a translator for some American staff in Werfen. (ii 20-22)

2. OKL Chistelle. Set up by Göring's orders and at Martini's instigation, had at the start only a few partially trained translators (in training at Chi), about 1937. Worked chiefly on Soviet radiograms which were characteristic of both airforce and army. Since unexpected difficulties were encountered von Longen often came to Chi for advice. Later von Lingen kept coming and was also available on the phone when Chi wanted anything from OKL Chistelle. Although the two outfits had parallel tasks there was no conflict and when necessary the two worked together openly to expedite the securing of accurate information. Fenner does not recall the heads only two men: von Lingen and Major Kupffer (earlier with Chi). (ii. 22-23)

3. OKH In 7 VI. The setting up of a separate outfit by the army at the wish of Gen. von Brauchitsch, but against the wishes of Fenner and Gen. Fellgiebel, was a misfortune. Chi had the only available trained personnel and not enough for its tasks, Now part was taken for Army and some intercept stations, hitherto controlled by Chi, were also lost. The actual cryptologic section lost but few men, other sections lost heavily. First chief was Capt. Kornatzky (captured at Stalingrad). Efforts of Chi to make some working contact with the Army outfit never amounted to anything. Whether this was due to the attitude of the chief, Capt. Wang, or to that of his superiors, Fenner could never find out. Chi was forbidden to continue working on foreign military systems. Fenner did continue some work because he felt that the Army outfit could not work certain problems satisfactorily. When Capt. Dr. Jung became head of army outfit, the tension lessened, and when Major Baron Osten-Sacken was head during the war Fenner even placed at his disposal solutions of Soviet systems, sent his men to OKH and generally aided in every possible way. Osten-Sacken killed himself after 20 July 1944 because under suspicion of participation in the anti-Hitler plot. When Fenner's men came back after their term of service contacts were not maintained (1942) but without any feeling. Osten-Sacken was followed by Lt. Col. Andrae. Another man at OKH was Baron Engelhardt (formerly with OKM), and Mr. Block, both formerly with OKW/Chi (RKM/Chi). (ii. 21-24)

4. Auswaertiges Amt. The cipher section of the Foreign Office grew out of the cipher service of Grand Headquarters of World War I. Ex capt. Selchow became head. Relations with AA were strained for some time because AA thought OKW/Chi should not meddle with diplomatic traffic. This was a pretext, really Selchow was afraid he would have to give more to Chi than he got in return. Chi kept silent the fact that it knew the real motives and advanced only the following well based arguments which strengthened its position:

1. If AA complains about Chi's deciphering diplomatic ciphers, will AA promise to turn over all its decipherments which touch on military matters?

2. Should AA decline, one might then discuss having AA turn over at least the content of such messages. Then, since soldier and diplomat read and interpert things in different ways, it might be necessary to find that such "contents" were not sufficient.

3. If it is asked that Chi confine itself to the relatively simple systems presently used by military units, how is it to be prepared to fulfill its primary duty: to be ready to read more complicated systems which must be expected in the future? Chi cannot content itself with working military systems.

Of course Chi knew these arguments would not make AA collaborate and were

advocated solely as a defensive measure in case AA tried to take away all diplomatic decipherment. In that case there was one more:

d. A diplomat ought not to be deciphering other peoples traffic; it might compromise his position; knowledge of the contents of secret messages brings him under suspicion of dealing with a "Black Chamber" much quicker than it would a soldier who can always say he has good Itelligence service. Reference was made to Hungary where all decipherment was in the hands of military personnel. No open break occured. Chi improved its intercept service and turned over thousands of diplomatic messages to AA, a real contribution, and Selchow now accepted the offer of cooperation and became an ally in case of attack from the other quarters. Workers of both outfits were allowed to talk matters over and since Chi could give more than could AA all went smoothly. At one time, to speed matters Chi personnel worked at AA on Turkish material. Finally, when Chi was bombed out, AA found space and the two agreed to keep in touch should they have to move out of Berlin. This was not possible when the time came. (ii. 25-29)

5. Forschungsamt (FA) des Reichsluftfahrtministeriums.

When FA was founded and some 33 persons went over to it from Chi, two or three of the moving spirits knew of the early friction between AA and Chi and realized that the question of "Competence" could be employed as a powerful lever since, as they claimed, Hitler had assigned the working of diplomatic messages to FA exclusively. There was some personal friction too. However, FA over estimated its omnipotence, the Reichswehrministerium had no notion of letting this work go. FA had no intercept service for radio but had claimed and obtained control of land line and cable traffic; also, despite more people and money, FA did not get ahead as fast with the decipherment. Selchow for months played along with FA but quietly asked now and then how Chi was making out. The more frequent request from AA for aid, indicated that FA was not able to supply what was desired. FA itself tried to get aid from Chi thus overlooking its claim that Chi was not competent. FA sent its traffic to AA and Chi but to Chi came only what FA saw fit to send and often Chi later got from AA material not supplied it direct. Persons at FA tried to get Fenner out but the exchange of traffic went on; no groups or other information was included in traffic went on; no groups or other information was included in the exchange. Fenner had no use for FA of for Goering, he considered FA a "private toy of Goering" which had no excuse for being save to further inflate Goering's vanity. (ii. 29-32)

6. Fenner knew of no other German cryptanalytic outfits but it is quite possible that the Security Police dabbled. Usually such systems were sent to Chi. A. Figl (formerly in the Austrian cipher section) appears to have worked with the police, Fenner is not sure. (ii. 32-33)

7. Note: despite the aversion of AA and Chi toward FA it is possible that FA did accomplish something. Their decipherments were never decently translated, sometimes the ambiguity was such that Hitler himself made inquiry to Chi as to the true meaning. Chief trouble was the "swelled heads of the chiefs". FA had a bad reputation, it meddled and made trouble in many quarters. It had a showy organization and boasted much, but performed little. (ii. 32-36)

8. People who left Chi for FA. 10 listed. (ii. 37-38)

4. Schapper was not "Chief" of any section at Chi. Schapper's dissatisfaction with Chi is treated at length: largely a Nazi matter. If anyone wants Fenner's views on this matter, they are set forth at some length. (ii. 38-44)

5. Fenner's life since the surrender is detailed; unimportant. (ii. 44-48)

~~TOP SECRET~~

#6. onnel of Austrian cipher bureau; steps taken to protect them when Hit marched in. Seifert, Bailovic, Feingart and Mauler were flown to Berlin; Seifert and Mauler came to Chi, Feingart to AA, but Bailovic was grabbed off by FA. AA also took over Bohuslav said to have joined the Party. Braunias later turned up in AA for a time. He began working against his former colleagues as "untrustworthy from the point of view of the Party." Purely for his own advancement. (ii. 49-56)

#7. A. Figl: Fenner does not know what has become of him, was about 75 years old. His second volume on Deciphering was not published because the Austrian cipher bureau objected. Figl did show it in Rome. Did not contain anything of great value. (ii.56-59)

#8. Relations with Huettenhain described at some length. Excellent. (ii.59-61)

#9. Waffen SS did no crypto logic work so far as Fenner knows. Members of the FA formed a special SS unit and pushed their own interests! (ii 61)

#10. Agents. Fenner never handled original messages. Most of the ciphers, usually book, were solved only after capture of the agent. If the books used were available, traffic could be handled at once, but often weeks or months passed before the right book or edition could be secured. Sometimes when luck was favorable, a net was worked and information about dropping of supplies &c obtained. Often word got back that an agent had been caught and keys must be changed. Perhaps 50 messages were deciphered in a week, somehowever were a year old, hence of historical interest only. The Wehrmacht was not in charge of arresting agents and did not control the situation, usually the agency spotting the station picked it up at once without waiting to use it, a practice of which Fenner did not approve. There was friction between Army and the Brown and Blackshirts. (ii 62-63)

#11. Gen. Staff studies on Russia: Knew little but did sometimes see studies of economic nature. Thought Haushofer, father and son, might have had a hand in these. Covered raw materials chiefly; Fenner not competent to judge quality, but felt they were carefully made (ii. 63-64)

#12. Fenner never knew of any find of a Yugoslav additive system in a cave near DRAVAR and does not know what system it may have been. (ii 64)

#13. Enigma, SZ 40, SZ 42 and SG 41. Hundreds of army Enigmas were lost so Fenner assumes US must have some. If he tried to write from memory without a sample machine he might get things mixed up so it would be better for an American expert to study the machines. Fenner does not know the other three machines; he refers to Huettenhain, Wenzer, Diploming. Rotsheidt, Dr. Lotze (WaPruef 7) and possibly Ministerialdirigent Georg Schroeder in FA. Huettenhain should know most about them. (ii. 64-65)

#14. Security studies. According to orders these should have been burned, either at Berlin, Halle or Werfen (ii. 65)

15. Fenner knows of no cooperation with Abwehr units on interception. No distribution list mentioned Abwehr and he never heard his superiors mention such a connection. (ii.65)

16. Chi's relation to Abwehr. Chi was founded as a unit in Abwehr, this subordination led to constant conflicts, Chi was nominally on Abwehr rolls while the radio men were mostly Nachrichtentruppen and the apparatus was under Inspektion der Nachrichtentruppen. In the small army of 100000 men this was not too serious since everyone knew all others concerned. Then to complicate things further came the T 3 (later Abteilung Fremde Heere) of the Truppenamt, which claimed it alone had a right to the decrypts of Chi. When FA was started, Gen. Fellgiebel wanted to free Chie from Abwehr but the decrypts were so important Abwehr objected and Chi remained as Gruppe IV of Abwehr but subordinate to In 7 as far as personnel and pay were concerned. When in 1935 Canaris became head of Abwehr and the FA was in project, the

TOP SECRET

situation became acute. Fellgiebel wanted to get Chi out of the Pokitical wrnagleings and now succeeded in getting it definitely in hands of Inspektion der Nachrichten Truppen (and its successor). Abwehr still got decodes but had not authority. (ii66-67)

17. Gen. Gimmler. Some derails; was an organizer and wanted to reorganize the outfit although late 44 was not time for such a step and he did not understand the work. Not a great success in his job. (ii.68-69)

18. NSDAP interference. Telephones tapped, letters opened. Fenner's dismissal was demanded because he had cussed out Goering "in Russian." Fenner was warned to be careful with his home phone because it was monitored, his packages were opened. (ii. 69-72)

19. Non Nazi officers and officials had the feeling that out of any three persons whom they did not know, one was a stooge of the Party. It was hard to pin anyone down since stoges operated under the cloak of anonymity; only one man from FA was discovered in Chi and he was transferred out at the first opportunity. Fenner was often warned by his superiors not to make any criticisms of the regime or of Hitler and his subordinates frequently came and begged him not to expose himself because it would be bad for all his people. From the VNs his people had some chance to size up the true situation. Fenner is not sure there were none in the outfit who were not noting all he might say but nothing ever came into the open and the Nazis never made any row. (ii.72-73)

20. Any practical cryptologist knows how often he need collateral information and how welcome it is to be able to get it promptly. The Archive was used daily. As Mr. Fenner recalls, the archive was consulted 7 times the first week, 70 the second, after that no record was kept the idea had taken hold.

The secret archive was presumably burned at Werfen; part of the VNs were burned in the air attack of 24 Nov. 43 (VNs of 40 to Aug/Sept 43) All older VNs (down to about 1937) were in the Army Archives in Potsdam and, in part, at Tirpitzufer 38/42. Fenner does not know what became of these. (ii. 73-74)

21. Mettig was with Chi OKH before he came to OKW/Chi. What he said about 5 place Russian traffic obviously has to do with what he observed at Chi OKH. Russia followed the international practice of sending all messages in five place groups so that anything else was probably an error and contrary to regulations.

(Fenner missed the point: When did 5 LETTER traffic first appear? he knew only 5 DIGIT apparently) (ii 74)

22. Fenner knows nothing of Russian teleprinters with cipher and also nothing of Russian agent traffic since he saw none personally. He did see the statements of some deserters and prisoners but could not dheck their statements for want of material. Ostensibly the agents used a 2 place numerical sustitution with keyword, only one value for each letter but reciphered with an additive. Example: Key: STALIN. S 01, T 02, A 03, L 04, I 05, N 06, B 07, W 08, G 09, D 10, E 11, 12, Z 13, &c down the Russian alphabet. Taking the birthdate 22.10.25 for recipherment base and a simple case of enciphering with this six digit number (mod. 10) would be one way; another would be deriving a Zahlenwurm from the date:

221025	x1	221025
	x2	2220410
	x3	6630615
	x4	8840820
	x5	1010501025
	x6	1212601230
	x7	1414711435 &c

From these sequences are derived the Wurm:

2: 204106630615884082010105010251212601230141471143 5.....
4 ,442451629367636248021111551127633386135315551825 78.....

Information regarding such systems reached Fenner's outfit "for information" but were not worked on there since outside its province. He assumes that Lt. Vauck worked over this information more carefully although not aware that Vauck deciphered any Russian ciphers of the sort after his transfer to Fenner's outfit in the fall of 44..
The example is only one of the myriad variants. Construction of the Wurm would only be learned after solution. Word about such ciphers had no practical value since one could never prove that the information was true. Col. SACHAROW formerly interned in the Haus Alaska knows Russian agent systems well, if anyone does. (ii. 74-76)

#23. Lists of abreviations were kept for years; little used in Fenner's section because few were met in the cipher texts and these were, or soon became familiar. Press and propaganda sections met more. Fenner's copies were burned in Berlin, probably the other copies were burned at Werfen. (ii. 76)

#24/25. Fenner saw none (ii.77)

#26. Getting maps of Russia was difficult. Captured material was worked over in a section of OKW since editions with Latinized names were needed. In 1944 the series was still incomplete and maps of all kinds were accepted gladly. Chi once got several from Finnland and work on these was rushed since they were only loaned, they were of East Karelia.
The Russians had old maps of the Zarist period with scales: 1:42000, 1:84000, 1:168000 and new maps with scales: 1:250000 and 1:5000000, 1:100000 (the most used Gen. Staff maps), also 1:250000 and 1:5000000. Only the western border areas and some east Asiatic areas had been newly surveyed, the other new maps were merely recalculated from verts into meters. Only a few unimportant areas were mapped for civilian use, mostly the maps were military. Fenner does not know how good the maps were.. Mostly they were in four colors, a few in more colors; the old Imperial maps were black lithographs and of no use for artillerists. New maps were supposed to be more exact, in particular the newly surveyed areas in the West. Most of the East Asian maps were from air surveys. Fenner had forgotten the name of the outfit which worked over the maps but an office with which he once had some dealings was in Lützowstrasse. All new maps were recalculated on Kruger-Gauss Coordinates and with Greenwich as 0°.
In general Chi used the atlases of Stieler, Velhagen and Kasing and of Ullstein; Also official maps (cable lines, high powered transmitters, intercept areas, &c. (ii. 77-78)

#27. Chi used the ordinary dictionaries: Toussaint-Langenscheidt, Schmidt, Sachs-Villatte, Pawlowski, &c. Most copies were private property of the men. A bookseller can give names &c. However, all failed to give the new terms of diplomatic policy &c. Kühn came to Fenner late in 44. The need for military dictionaries was great, those issued before the war were out of date since military vocabulary develops faster than that of scholars or diplomats, and soldier jargon affects them even more than technical advances. All translators and all in contact with the enemy needed dictionaries. To unify the work for preparation, to save paper (shortage) it was asked that all military dictionaries be entrusted to Fenner (he had the best trained philologists available anywhere) and nowhere else was so much material at hand for checking. The project was approved and Kühn and his handful of people assigned to Fenner. Early 45 an English dictionary (including slang) was lmost through the compilation stage proffsheets were being read. A russian military dictionary was in progress. The material was burned at Werfen but Kühn may have saved some private notes. Fenner though the books were promising for postwar use. (ii.78-79).

28. [illegible] my impression, and I am convinced [illegible] at the secret archive (Dissem[illegible]n of information) evaluated the VMs carefully and according to com[illegible]rinciples, otherwise inquiries would not have come in from outside off[illegible]. I know, for instance, that Gen. Staff once wanted to know whether from VMs or other sources we knew anything about Russian preparations for war. There was a time when an answer would have taken 3 days to prepare and have been spotty but this time a full answer was ready in 3 hours. The archive gave only factual information with no attempt at interpretation. At a time when propaganda was confusing to everyone such a source of reliable information got firmly established in short order. As long as the archive was under Fenner's jurisdiction he and his workers tried to make it a source of truthful information which could be relied upon absolutely.
Fenner did not know the distribution of the VMs. Lt. von Kalckstein or, perhaps, Dr. Schaedel would know most on this subject. His outfit merely informed of the number of copies required, it did not control distribution or even pick out specific numbers needed for any particular purpose.
Reports were, as already mentioned, put out monthly at first, then from about 1927 only every 3 months and in 5 copies. From 1933 on only annual reports, 2 copies, were prepared (a 3rd copy was made in rare instances.) (ii. 79-80)
29. Fenner knew no American or English patents for cipher machines. When negotiating with Siemens early in the 20s for construction of a cipher machine he heard of Hevern inventions and Chi had a prospectus which, like most, gave no vital information. Chi never heard whether the Electric Hebern was ever built. He does not know whether American or English patents ever helped or inspired German inventions. He did not know foreign patents well enough to be certian on this point. (ii-81)
30. Patents were issued by the Reichspatentamt if the conditions were fulfilled. This was determined by the examiners. Any N.Y. patent attorney can give details. If national security called for secrecy, application was made for a secret patent. The chief difference was that the letters patent were not published and only one man handled these documents, one approved by the Patent Office. Enigma had secret patents, also Siemens and other firms. When the authorized representative, say Wanzer, came to the proper officer of the patent office he was shown the latest list. It is erroneous to think that possession of a patent means possession of the knowledge needed to make it effective, in Germany the ideas were patented and it might be a long way to perfecting the device. The Waffenamt did all writing concerning patents for cipher devices. It made application, paid the fees, including annual fees for the 28 years of validity. Of course Waffenamt kept a list of its patents but Fenner does not know where or what became of such lists. (ii.-81-82)
31. Dr. Weisser and Councilor Schulz could tell best who first solved the American strip system. Fenner's recollection is as follows: the courier brought from Rome a description of the solution which rather astonished Fenner's outfit since it was one of the toughest problems. Chi did not believe Rome could have done it independently but the solution worked. At the Foreign Office they were working intently on the problem at about the same time, later with success. He thinks the primary solution was obtained in Rome, whether by purchase or not Fenner does not know. Then Chi worked it over carefully, then AA and Helsingfors. It was known then in the order: Rome, Chi, AA and (FA?) Helsingfors, Budapest, Rome and Tokio were not informed of our success since we did not expect any advantage from their collaboration. (Should the break come after Helsingfors or where??) (ii. 82-83)
32. Schluesselscheibe and Schluesselkasten.
Mr. Fenner assumes knowledge of the double transposition and other transpositionssystems used by the German army in World War I, also the Enigma machine

(lamp model), and the relative advantages and disadvantages of the two systems.

These had been discussed over a period of 20 years with the idea of creating a device for troops which would have the following properties:

a. light weight and small compass,
b. absolute freedom from operating failure,
c. be easy to operate,
d. derive the cipher or plaintext by a simple rule, certianly in one operation.
e. yield undecipherable ciphertext,
f. have a simple distribution of keys,
g. be simple to administer.

None of the many, often very clever, hand systems satisfied the demands. (the very intrguing French small "Signaltafel" (code) with some 1000 groups and numerous blank spaces was excellent, as experience distribution facilities.) Some other course had to be pursued. Likewise the numerous lay suggestions for use of discus of line slides had to be rejected, even when for greater security the cipher was a funciton of the plaintext. In such cases an error continues as its own function throughout the length of the message.

The only idea which turned out to be theoretically and practically of value was the use of a substitution system with aperiodic progression but with a long period. The technical problem was to mechenize this idea. For clearly with a primitive linear slide

Plain myiunbshvtalxdcjgrkcpzfwoe
Cipher pucivdznqoramyjbwxfskelhtgpucivdznqo..

and an aperiodic numerical key, e.g.
4132031526410.....43103
a cipher can be derived which cannot be solved analytically although it goes back to the Middle Ages (Tritheim 1462 to 1516) (Note: According to Vigenere).

If it were possible to use such a practically endless/sequence of digits to drive the red disc then the desired device would be achieved to all intents an purposes.

However the minimum length of such a device had its limits: if the alphabets were to be changed, then the cells would have to be capable of inscription. However, with a cell width of 1 cm the minimum length would be 52 cm since one alphabet must be double. This would be intolerable.

A way out was found in subdivision of the two alphabets thus:

(black) myiunbshvtalx
(red) pucivdznqoramouci.....m
(red) yjbwxfskelhtgyibw.....g
(black) dqjgrkcpzfwoe

This let the device be reduced to a length of some 30 cm but an unforseen disadvantage lay in the coupling of two black and two red letters.

Working out the driving mechanism in such small compass was even more difficult.

A drawspring supplied power. It was released by a pushbutton. When at rest the movable slide had to be firmly locked. The final step of the slide, which was pulled out by hand, had to unique. All this called for carful mechanical construction.

To mechanize the aperiodic motion recourse was had to socalled pinwheels, such as are used for the same purpose in the Hagelin, and the structurally necessary gearwheels. All these drive elements were so easily reached from the

betwe[illegible] f the device that even the clumsy fingers of a soldier would operate the individual parts.

Fenner no longer recalls how many pinwheels and gears the device had, however, 4 cogwheels with 17, 19, 21 and 23 teeth respectively would yield a period of 156009 steps. He assumes that at least 5 cogwheels were projected and the same number of pinwheels, but the number does not matter for the theory.

The total period is shortened by the effect of the pinwheels. Also there are favorable and unfavorable pin positions. The problem of the favorable pin positions was subject of special consideration. In practice each clerk had to possess a table showing "forbidden" positions. Such a table had already been prepared at OKW Chi.

Experimentally a Menzer slide about 17 cm long, 8 cm wide and 6 cm high had been constructed, with a much shorter period. The Wanderer Werke had been intrusted with the construction. The army did not get beyond the experimental stage and Fenner never heard that the first set was ever tested by the troops. All experimental models were useless because the device was always jamming (Klemmte).

The intention was to write in a new alphabet at least once a day and to use a new setting of the pinwheels and cogwheels for each message. The clerk was to have free choice in this last so as to guarantee as much individuality as possible; naturally this entailed sending an indicator group. No completed Instruction and Keying Manual was seen by Fenner.

Mr. Fenner thinks the device would meet current cryptographic requirements but no thorough analysis had been made to his knowledge. (ii. 83-86).

#33. Poor phrasing of the question, coupled with a spelling error, caused total misunderstanding of this question. (ii. 86)

#34. Collaboration with Japanese was really impossible since Hayashi was cut off from Tokio and little material got back and forth. The main interest was to determine whether systems solved on the west front also appeared on the east front, however, Berlin never found out what the Russians did use in Asia. Toward the end, Hayashi asked to be informed, since he was almost entirely in the dark about events; he was geven carefully selected VNs from time to time but that was all. (ii.87-89)

#35. Fenner seems to have had no knowledge of Schauffler's "wissenschaftliche Berichte". Merely assumes that anything Schauffler put out would have been worth while. (ii. 89-90)

36. Fenner says he knew no more about secret inks than one could get from an encyclopedia or childs book on magic. Once looked through a microscope at a microfilmed map of Germany which was shown him as demonstration of present day technique. Both were out of Chi's province. (ii 90-91)

#37. Fenner thinks there were probably messages of the Lublin govt. among the many Polish messages decrypted but does not know. Assumes they would have been substitutions with additive, the latter probably from tables.
Berndt would know best, then Huettenhein who would have conferred with Berndt on the encipherments. (ii. 91)

#38. A few B 211 machines reached Chi. Now. He knew no other French machines. Thought the printing model Hagelin was used by English perhaps. There was an erroneous impression about that OKW/Chi had solved the B 211 but this is false. Huettenhain's talks revealed that the B 211 might be solved under certain circumstances. It may be that OKH Chi really did get a few solutions. (ii. 91-92)

39. Fenner knew no American cryptologists by name. From Yardley's book it was known that successes had been scored in World War I and it was assumed that Americanwouldtuse this source of information again. An American newspaper had an item about an organization which located and determined the nationality of unknown transmitters very speedily. Since such determination is out of the question without reading traffic, he assumed there was a large deciphering outfit. Even if this were an exaggeration, it must be assumed that USA was doing something in this line, any such effort would not be a bagatelle. Later from Africa came unconfirmed rumors of a cipher section with IBM machines. After the landing in France a secret document of the USA signal Corps was captured somewhere. In this report the question of decrypting is raised. Fenner got the impression that American military circles, like the German, sometimes questioned whether decryption was sensible. He knew by experience such questions which suggested that the questioner regarded every decryption as a plant; other less intelligent people would ask: why don't you decrypt only the important messages? The American critic comes to the laconic conclusion: either the decrypted message contains the truth or none at all. Such a statement could only have come from a man who understood the technical basis of analysis and had often been convinced of the relation between a decrypt and the truth. No there was no doubt but that America had a official cipher outfit.

Nothing certain was ever heard about English work but it was assumed certain that it was in competent hands. When England tried to get the Turks to use English systems, Germany heard of it and inferred that England must be reading Turkish traffic, at least. If Turkish, why not others which were no more difficutl? After World War I there was an unconfirmed rumor that Former Russian naval officers who had worked on systems of the German Baltic Fleet were working for the Kremlin. From the gradual development of Russian systems from fairly easily solved to insoluble enciphered codes with one time additive it must be inferred that Moskau had serious people at work, monitoring their own systems and replacing them when they might be used to the point of breaking. Reports on the strict selection of personnel for the 7th section of the Gen. Staff suggested that security was receiving much attention. Since Fenner's experience shows that the analyst is the one who bolsters up the country's own cryptographic means, it was certain to him that moscow had a cryptanalytic outfit.

Captured Russian instructions were so clearly thought out as to indicate that much analytic work had been done, otherwise no such cleat use of terms would be possible. The similarity between siplomatic systems and those of the higher staffs suggested a common control. (ii. 92-94)

40. Just before the war one of his men brough a clipping from a French journal with an ad of a course in decrypting. He thinks the price was 20 francs. For security reasons no attempt was made to connect. (ii. 95)

41. Menzer came to Chi in 1933 after 12 years in Signal Corps where he had risen to Oberfunkmeister and where his duties were to lick and seal hundreds of envelopes. After testing him, Fenner though he was too good for such a job and menzer was transferred to Chi. He took the first course in cryptology, got outside aid in math. and got acquainted with vrious aids, worked on suggestions that were offered and was gradually attracted to the development of mechanical aids. He was also assigned to make small hand systems for the German forces. He was not gifted at decryoting, even a simple substitution was uncomfortable for him, but constant application with rigid criticism and

a systematic sera for truch widened his horizon while his knowledge deepened. He took up the Enigma then in use and checked the security of German systems. He showed that the Enigma was used wrongly, as was known, he worked out his studies in the proper form, never asserting more than he could prove. From 1938 on he busied himself more intesively with the development of ausiliary devices to aid decipherment, always asking what do I expect of this gadget, what is it to do? His first attempts were primitive: Working with some strips of wood he obtained a recurrent periodicity but with no money, no grand result could be hoped for. There was a lot of talk of the need for a device to locate and record repeats; some funds were made available and some mechanics arrived but then it appeared that the technical knowledge of a former radio man was not adequate, so Menzer was put under Huettenhain and graduate engineer Rotscheidt transferred to the section. From their collaboration resulted the devices mentioned above. There were long periods where Menzer worked entirely on hand systems. He was responsible for the so called "Heftschluessel" (pad key?) which was cancelled shortly after its introduction because of compromise and because it was not as secured as one had thought. "Some impossible mistakes proved possible". This resulted in the realization that our own systems must be checked more carefully. In this Menzer proved very useful and reliable. Before the war Fenner was troubled because the Abwehr was using systems he had not checked, and during the war occasional requests for systems strengthened his suspicion that not all was well with the Abwehr cryptography. Menzer was assigned to go to the Abwehr and, despite any opposition, to check all systems and replace poor ones with some Fenner had checked, This was Menzer's last big task, and he did it to Fenner's complete satisfaction. Menzer's strong points were: small hand systems and small auxiliary devices; criticism and evaluation of systems. His judgment was good and he considered all sorts of minor weaknesses. (ii 95-97)

42. Yes, He recalls talking with Paschke of AA about the end of 43 about some traffic, 30 letters long with some sort of indicators. Source was not recognized and anyhow the traffic was outside his province, so no study was made. (ii. 97)

43. Fenner never saw the Olivetti teleprinter. Huettenhain said it was not thoroughly developed; the constants outweighed the variables in the machine. (ii. 98)

44. Fenner knows nothing. Suggests asking the former Russian officer SACHAROW who should be well informed (ii. 98)

Volume III.

1. Dr. Lutzen did start a study of Finnish systems in 1940 but this was dropped in favor of more important work. No results. Though transposition was used. (iii.-1)

2. In the late 20s and early 30s Borsi Hagelin developed a cipher machine based on the principle of a practically endless Tritheim. He accomplished this by a number of cogwheels, the number of teeth on the several wheels being prime to one another (11, 13, 17, 19, 21, 23), and so called pinwheels the purpose of which was to let the period run along in irregular steps. A third aggragate, the basket, served to substiutute the alphabets immanent in the machine. This device, which was about 20 x 15 x 8 cm in size, was built as a tape printer. Pressing a hand lever caused the entire mechanism to advance to a certain number of steps. The alphabet wheel had to be set by the left hand, then there appeared alongside in a slot (?) the appropiate cipher letter after operation of the lever. The device was cryptographically excellent but had the disadvantage of working relatively slowly.

[illegible] not secured because Hagelin is reported to have [illegible]ed over a mill[illegible]marks. He later told Fenner that his machine was being built in France under licence.

Some years later it was apparent from advertisements that Hagelin had improved his machine, he had introduced a keyborad, similar to a typewriter, and had, as Fenner recalls, both a straight mechanical and an electric model. Since Chi and the Waffenamt had since 1935 some ideas of their own, they contented themselves with what information they had and did not buy any of these devices for study. (Due to the exchange rate any such purchase would have been very difficult).

In the summer of 1940 some machines were captured in the West which were recognized as automatically printing, electro-mechanical TEKNIK devices. The base plate was about 40 x 40 cm, the height Fenner estimates at 15 cm. He knew of two such machines and assumes that the Waffenamt also got several (WaPruef 7). None were intact and Fenner no longer can say whether they were page printers or tape printers or whether they printed both texts simultaneously for control purposes. This was of secondary importance to Chi. What was important was that to derive the elements of the cipher text elements of the already known small Teknik were employed, viz. :

1. cogwheels, the number of teeth being prime to each other
2. pinwheels.
3. a basket with riders.

Something new was that wheels, similar to those of the Enigma, had been introduced to effect the substitution. As Fenner recalls, a dry cell furnished current although he thinks there was a cable for connecting to an outside power source (transformed from light circuit). He no longer recalls the installation of the several parts and their interaction. (Since no traffic which had plainly been enciphered with these machines, was at hand and he did not know whether they were used by the French or the British, the cryptologic interest was satisfied). However, the analysts and technicians were much interested in one wheel which was missing in every machine captured, it was about 4 cm long and 3 cm wide as Fenner recalls. It was located between certain electrical poles after the fashion of the small Enigma wheel and was thought to have significance as a supplemental security factor. He does not recall how many poles this body (wheel) had on its face. At that time he assumed there must have been a large number of these secret wheels and it was clear that the apparatus would not function without one. Hence the machine could stand out open on a table but when it was to be used some one (officer or official) had to insert such a wheel. Fenner asked that search be made in all stores and factories of the occupied territory for such wheels but none were found. Accordingly none of the machines could be put in shape to operate and study.

However, one thing was clear to Fenner, Huettenhain, Rotscheidt and Menzer, namely that Hagelin had a good start and that the machine must be theoretically very good for a permanent location. They could not set up any rule for the solution of individual Teknik messages; of course they did not know either what defects the machine might have or whether it was free from "troubles".

It was too late for the machine to have any influence on German developments.

When Menzer left Fenner's group late in 1944 Menzer took the machines with him and Fenner does not know what became of them. Menzer tinkered with one for a long time but Fenner thinks he would have been informed had anything resulted.

The machine appeared very solidly and well built and betrayed excellent workmanship. (iii.1-5)

#3. When after the first World War Poland set up diplomatic mission abroad it took up familiar means for secret communication with those missions.

[illegible] Chi began working on this traffic several systems may have been in[illegible]ced and replaced so that Fenner can say nothing about such earliest types. But it is possible that the traffic worked by Chi early in the 20s represented the earliest systems: 5 digit groups with repeats within and between messages of the same day but no repeats between different days. The repeats were always 4 digits long or a multiple of four so there was no doubt but that the basic code had 4 digit groups. The parallel passages used to study the encipherment showed affinities of indisputable regularity, for instance, if on 1 Oct. a parallel passage read 4354 there would be found on 2 Oct. 1061 9066; likewise if yesterday a frequent group read 8579 there would be today a group 2693 with about the same frequency, i.e. appearing about as often porcentually. On the basis of these observations and dozens of confirmations it was natural to assume that a four digit code had been enciphered with a simple substitution table, say something like the following:

2 Oct.

0 ? 1 ?, 2 ?, 3 0, 4 1, 5 6, 6 ?, 7 9, 8 2, 9 3.

Working over the collective traffic of each day led to the same phenomena. Hence the assumption was confirmed and the next step could only be to render homogenous the heterogenous material, i.e. to give it a form as if of the 10^3-1 arithmetically conceivable permutations of the substitution table only one and the same had been used each time. This process was called reduction to the relative basic code. It was accomplished by using as large and ungarbled collections as possible, one of these texts being regarded as "unenciphered" and the others being reduced to that. The reduction was relatively mechanical and since it is assumed that cryptanalists all over the world use the same method as suggestion will suffice.

The following sheet shows a section of the count of the collection taken as basic code in four places (black); the count of the second collection, likewise 4 place, (red, and the count of the third collection under the same conditions (blue). If black 1365 is the most frequent group of collection 1 and 0128 the most frequent of collection 2 while 5431 is the most frequent in collection 3 and the three groups may correspond to each other, we can already make the following reduction:

black	red	blue
0		
1	0	5
2		
3	1	4
4	6	7
5	8	1
6	2	3
7		
8		
9		

It is obvious that through other comparisons additional values will be found so that with adequate material all messages can be reduced to "black" and the results used for code breaking.

That is how the 4 digit code enciphered by simple substitution tables was solved thus proving that such a system in not secure enough for the present day needs.

Although a system had been chosen which in and of itself was insufficiently secure for state secrets the solution of the daily changing encipherment was further facilitated by the fact that Warsaw itself made a change not necessitated by the system but due solely to thoughlessness and convenience. In Com-

0		28 28 28 28 28 17 28 03 28 03 03 28 28 28 17 (red)					82 82 82 82 82 0 82 (red)	
1				65 37 65 65 65 65 65 18 65 65 65 65 65 27 65 65 32 65 65 65	56 56 56 56 56 0 (black)			
2								
3								
4								
5					31 46 31 31 31 72 31 31 31 31 31 57 46 31 31 31 (blue)			13 13 13 13 13 0 14 (blue)

(black)1365 (red) 0128 (blue) 5431

1456 (black) 0682 (red) 5713 (blue)

-TOP SECRET-

pl... the progressive daily keys of a ...hed systematic sequences were noted wh... made possible the reading of traffic on sparsely filled days and also the reconstruction of the substitution tables even before a single message for the day had been received.

Obviously the tables for each month were printed on a single sheet. The official entrusted with preparation of the tables made it easy for himself and omitted the all essential feature, i.e. random selection which would have excluded any unintentional though physocologically comprehensible system. Thus the tables looked somewhat as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	6	9	3	9	1	5									4	4	2	2	0		3		5	1						
1	0	3	9	1	6	1	5					4		2	4	0	2	3		2	1		1					4		
2	3	0	1	3	5		1	5			4		2		0	4	3	2	0	1	3			1			4			
3	2	1	0	5	3			1	5		4	2		0	5	3	4		1	0		3			1		4		2	
4	1	2	5	0	9	3			1				0					1												
5	4	5	2	8	0		3			1				0					1											
6	5	4	6	2	7	0		3			1	0						1												
7	9	6	4	7	2		0	4	3	2	0	1					1													
8	7	8	7	4	8	2	4	0	2	0			1		1															
9	8	7	8	6	4	4	2	2	0	3	5	5																		

Systems of this and other types occurred by the hundreds and were the rule, whereas unsystematic tables were the exception. And even though the system here in only partial, it nevertheless facilitated decipherment in countless cases for once part of a month had been solved the worker knew approximately what the table for the next day would look like.

After this system had been used several years it was replaced without notice by a new 4 digit code enciphered by an additive (Zahlenwurm). (Fenner cannot date precisely without records but recalls that at the time of the "Letterbox conflict in Danzig" the new code had been in use several months).

Ciphertext critique, i.e. examination of new cipher texts without making any counts, yielded a different picture. The number of parallel passages had been reduced materially, again the length was four or a multiple of four, hence, the basic code was four digit, and this was confirmed by the fact that the interval between parallel passages was also a multiple of four. A frequency count now showed a perfectly colorless picture with virtually every digit of the cipher text appearing almost equally frequently procentually. Since it was known that an additive sequence of sufficient length produces this effect, such an additive was assumed to be used. The socalled phase or interval having been determined from the parallel passages, the next task was to pick out enough homogenous material enciphered with one and the same additive sequence. The introduction of the additive sequence (Zahlenwurm) meant a great cryptographic advance. But again Warsaw felt perfectly secure. This was subjectively comprehensible but could not stand up against objective criticism. The sequence was short and was in use so long that regularly enough traffic could be assembled to permit solution. For this the usual difference method was employed, this is based on the fact that like differences of two groups at the kth and $k\ n^{th}$ positions of the additive sequences indicate the same code groups:

	.....k.....	k.n.....
	3456	4567
	....	....
	....	....
	7322	....
		....
		8433
difference.	4976	4976

-TOP SECRET-

Warsaw is also the difference between plain code groups 2345 & 211.

Since reduction to the true basic code is possible only in the rarest cases, reduction is usually to a relative code, this is continued until enough homogenous material is assembled to allow attack on the problem of code breaking. The Polish correspondence was always so lively that there was always enough material. Once more the measures to safeguard state secrets were not adequate. In spite of the introduction of a modern system the mistake had been made of sending too much traffic with too short sequences so that the system compromised itself.

It must be assumed that later some competent critic appeared in Warsaw who recognized and spoke of these weaknesses of the system, possibly an officer, (Lt. Szczezinksy?), for the next improvement was a lengthening of the additive sequences. The use of a 40 place sequence bespoke lack of imagination; 40 is a multiple of 4, after the sequence has been run through the next group begins with the first digit of the additive; a sequence of 37 on the other hand with a 4 digit code would only repeat thus after 4 x 37 position, i.e. every 148 steps. When Warsaw became aware of this the sequences were altered; soon thereafter sequences of much greater length appeared, even up to 200 digits or more. This was an advance for it always happened that messages were sent which were shorter than the sequence and, unless much material was at hand, many messages remained unread. It is well known that anything which is theoretically correct must be correct in practice. If contradictions are found, either the theory is false or errors have been made in practice. The theory of the additive sequence requires, of course, that the sequence shall not always be applied at the same position in the intermediate text. In practice the picture was quite often different! The decipherers got the impression that the sequences were kept in drawers and were mere force of habit. When this was noticed the sequences were in use for relatively long periods of time, how long mr. Fenner does not recall, but in any case long enough to permit solution of the encipherment as a rule. Subsequently at least one fault was eliminated: the period of validity of the sequences was shortened.

The result was that traffic that could be solved shrank constantly and fewer and fewer messages were read. However, Warsaw could still not decide to give its inherently excellent system a stability in practice equal to its stability in theory. Only during the final months before the war was this level attained although it would have been possible from the time the additive was introduced: now the sequences are different in each direction on a circuit, i.e., the sequences used from Warsaw to London are never the same as from London to Warsaw; the sequences are so long that rarely does one begin to repeat within any message; they are of such short validity thar rarely does one obtain enough material to permit solution of the encipherment. For months before the war Chi was unable to decipher a single Polish diplomatic message. With that Warsaw had met the requirements for a modern government's secret writing: its nature was known, its weaknesses were known, but it was employed with due regard for its theoretical values and therefore protected the secret from every unauthorized decryption.

When war came and the Polish government in exile began to send and receive messages it soon became apparent that the lesson had not been forgotten. The additive sequence was retained but in view of the difficulty of preparing and distributing these the choice fell on sequences which could be derived from extensive tables. Surely the government realized that this would be risky if used for a long time but it may have been beyond its power to do better under the circumstances; anyhow eventually great numbers of messages were read. Change of the basic code and of the tables made no essential

change in this result but it would be a mistake to suppose that solu. n of these messages was an easy matter. Weeks passed before enough homogenous material could be assembled and the personnel shortage at Chi made it impossible to handle this traffic as had been done in peacetime. To get results ausiliary devices had to be employed such as differencing machines and Hollerith machines if decipherment were to have any practical value. This should not be considered a point in favor of the system since the modern cryptographer must figure that the modern cryptologist will attack his systems with machines which save a lot of writing. Moreover the rule holds that every cryptographic system has an imminent degree of security which must not be overburdened. When the limit is exceeded is a point which cannot be determined at the time of introduction and, more often than laymen will assume, is not recognized by the user since he rarely knows the total use made of the system.

The system known as "militpologne" was also worked and the encipherment was solved. Fenner can give details only with reservations today: a 4 digit code enciphered with simple substitution tables, no great problem per se but rendered very difficult by the dearth of traffic. So in this case everythin g was known but the code could not be solved because the limit of safety was never reached, let alone exceeded.

That Warsaw was not idly resting on the laurels of the virtually insoluble endless additive sequence was proven by some captured items: Military-political codebooks in several languages for carrying on correspondence in Polish, French and Romanian. From other codebooks and encipherments it was recognized that Warsaw was trying to prepare for any eventuality. Even the external appearance of these documents showed that attention had been given to quality of paper, binding, &c. Hence the entire cryptographic setup evidenced a certain substantial quality.

It should be remarked that the philological solution of Polish codes was not made easy. A comparison with French codes, which were also 4 place as a rule, may be enlightening. The French carefully encoded every stem and every ending and insisted on precise use of grammatical forms, the Poles went to the other extreme, they often give only the stem and assume that the decoder will get the right meaning readily from his general knowledge of the political situation. That was probably true but the crypologist is greatly hampered in his code breaking by such procedure. Whereas an ordinary French diplomatic code can often be read after some 1500 groups have been recovered. 2500 groups would not be enough in the case of a polish code. This observation deserves mention as proof that it is important to use an encoding procedure which will cause enemy analists additional difficulty.

However, it is true of the cryptographic activity of the young Polish state that even where there was certainly no dearth of advisors the development of cryptography does not progress by leaps and bounds but rather is bound organically to an organism man, whose spiritual eye can, to be sure, in happy moments penetrate to great depths, great heights and remote distances, but still is not able to compel his fellow man to do what is sensible. (iii 5-16)

#4. The question shows a misunderstanding. Fenner said that Huettenhain saw the Olivetti machine and reported there were so many Italian navy men about that he felt it was sponsored by the Italian navy rather than by the army. No mention was made of the American navy (iii-17)

#5. Chi[illegible]ved Russian army systems cu[illegible]tly from World Wa[illegible]on and followed the development from simple substitutions to codes with additive encipherment. Which system was used in maneuvers of 1930 Fenner cannot possibly recall. He has become acquanted with hundreds of systems and kept as few as possible in mind to a degree that would permit recall of details 16 years later. If it were a code, it must have been OKK 2, since OKK 1 was supposedly set up in 1929. It was probably a 3 place code with part of the digits enciphered by tables. Such a system would fit about that period. (iii-17)

#6. Menzer's discoveries of weaknesses of the Enigma. Fenner was not actively concerned with the latest developments and in case a new model was made during the war he cannot give many details, he assumes the principle was not changed. He assumes that at least one perfect specimen is in Washington since many were lost and proposes, in case the bulbs work, the following experiments:

1) If in any wheel position key A is pressed and K lights, then if the same wheel position K is pressed A will light up. Further experiment would show that the letters are tied two and two in a reciprocal relation. This means there are "reciprocal substitutions" in the Enigma system. The number of substitutions (Caesars) with a 26 letter alphabet is 1x2x3x....x25x26 or 26!. This is an inherent weakness of the machine which cannot be overcome since it is conditioned by the construction, the wirings and circuits. However, in the entire Engima system there are only 13! different substitutions. If one of these can be solved then, even during solution it appears that each solution gives two values. If cipher a equals palin k, then in this position cipher k equals plain a. This weakness aids in the complete solution.

2) If there is a machine available with three ratable wheels between two fixed wheels, then the complete cycle is exhausted after 26^3-26^2 or 16900 steps. The movement (next few words do not seem to make sense, perhaps something omitted in transcriting) instead 26 x 26 Caesars (substitutions) are skipped. This results in a shortening of the period although the progressionis disturned.

3) Assuming that the machine may be operated for a day with the same wheel position and "Rastenstellung" and that all messages are set up in exactly the same wheel position, say all with the setting 010101, solution of such messages would cause little difficulty if there were some 70 of them. Less would suffice if the analyst had some experience and a method. To avoid such a piling up of messages at one point in the wheel period all messages ought to be distributed evenly over the period. This can be accomplished for traffic from one point but not otherwise. It is most advisable to prescribe for the offices the choice of arbitrary settings since probaility indicates that then the days quantum will be so well distrubuted over the whole period that no dangerous pile-ups will result.

4) However, this security was not adequate for no one can say how great the daily volume of traffic will be in a future war, all predictions were quite without bias of fact and hence unadequate. The ideal would have been to be able to make current permutation of the circuits, e.g. if one could interrupt the leads of the fixed wheels at the right and constantly change the poles. This consideration led to the "Steckerbrett" (plugboard) in the front of the machine. Without bridging by jacks the machine works so to speak in normal fashion.

G- E cipher machines. Development was in the hands of the Waffenamt. Chi was, to be sure, concerned with criticisms and analysis but only gave suggestions, it could not construct any. The Enigma was considered outmoded although secure when correctly used. The Geheimschreiber (G-schreiber) was modern but not mobile enough. All plans for new developments were doomed by the end of 1944. No more practical work could be undertaken. (p.3.)

Fenner I-206

Organization of Chi 1939-1944....

Nothing is so wrong as to assume that your opponent will not notice and utilize the weaknesses of any system. Hence Chi assumed as a matter of principle that complete Enigmas would be captured along with instructions and at least a few keys and that the enemy would have radiograms. It was also self-evident that even with correct use, chance - which cannot be predicted and can only be recognized when it occurs - would give the enemy the possibility of deciphering some individual Enigma messages. What must be avoided was that the enemy read the traffic currently.... Provision was made that the message key chosen should be sent disguised so as not to facilitate the work of the enemy cryptologists. If they were already deciphering they would have to hunt through the traffic to find messages that belonged together. Chi assumed that this process would take so much time that no tactical use could be made of the messages after they were deciphered. That is all that was asked. (p. 30)

Fenner I-206

Fenner I-206

There were further investigations climaxing in the question whether the Enigma message could be solved when the machine and keying instructions were known. The analytic answer was - yes; intentionally I do not say the theoretical answer, since a correct theory entails a correct practice, otherwise there is an error in theory or practice. So the answer was that a single message could be read given the proper machine; wheel position and all other settings may be unknown, it is only essential to have the machine with the wheels actually used in enciphering. However what was done in a simplified experiment would in reality have called for a lot of people or a tremendous number of machines (cryptologic aids) so that once again one need hardly count on practical results under normal circumstances. (p.3 31

Assuming(one) had the machine used and messages enciphered with it,(One) would assume, let us say, the word "regiment." This plaintext word would be tried with every successive group of eight letters, resetting the machine until at the proper place in the message "regiment" was obtained, with intelligible text before and after the word. Obviously this would call for much time and effort and afterwards would have to be repeated with any change of wheel position or plugging. Chi thought that in modern warfare no one would be patient with such loss of time in decipherment and so felt that, correctly used, the Enigma was secure enough. (p.31.)

5) If you key a message in a predetermined setting without use of the jacks and then repeat using a bridge let us say connecting A and K then the two texts will in the main be alike, this experiment will suffince to prove that a single plug connection is not enough to produce any marked disturbance in the substitution sequence of the period. Even with two or three plug connections the changes are not great enough to insure security. Since in figuring the connections combinations are encountered, the maximum is not 13 but some lesser number.

6) Nothing is so wrong as to assume that your opponent will not notice and utilize the weaknesses of any system. Hence Chi assumed as a matter of principle that complete Enigmas would be captured along with instructions and at least a few keys and that the enemy would have radiograms. It was also self evident that even with correct use chance-which cannot be predicted and can only be recognized when it occurs-would give the enemy the possibility of deciphering some individual Enigma messages. What must be avoided was that the enemy read the traffic currenty! It was clear to Chi that Enigma messages with like or very similar key settings must contain parallel passages which would be a weakness since they would permit working kindred (affine) messages successfuly: it would only be necessary to superimpose these messages correctly then all elements in a column would be enciphered with the same alphabet (Caesar). For example:

.....aldefrc.....xdert.....cafhjk.....
.....ligtfde.....sdert.....vgftrea.....
.....aldfrcc.....bhiklog.....
.....xzzefrc.....cafholj.....

It must merely be remembered that due to the dropping out of certain alphabets (Caesars) the cipher elements of all columns across the entire width need not come from the same reciprocal alphabets. Hence the possibility of the occurrence of such parallel passages should be avoided as far as possible. Parallel passages arise through the use of like letters at like (identical) positions in the period. Like letters come from the choice of the same words. The military language is poor in words! Such words as enemy, hostile, attack, ammunition, &c recur again and again. In these words the most frequent letters also appear, e.g., e, n, i, r, s, t, u, d, a, h, b. If plugging is used it is well to plug these frequent letters.

7) Now the number of practically possible plug combinations is structurally limited. The plugboard is close to the front cover and not many cords can be used in the limited space, therefore recourse was had to permutation of the wheels. The 3 movable wheels can be arranged in 6 ways so that with respect to the output sequence five new sequences are possible. But each new sequence means practically a new period of some 17000 steps so that there would be a period of some 104000 steps for a day which was considered adequate if the plugboard was used properly. Of course one thought of introducing entirely new wheels from time to time, that was the practice. And of course provision was made that the message key chosen should be sent disguised so as not to facilitate the work of the enemy cryptologists. If they were already deciphering they would have to hunt through the traffic to find messages that belonged together. Chi assumed that this process would take so much time that no tactical use could be made of the messages after they were deciphered. That is all that was asked.

8) There were further investigations climaxing in the question whether the Enigma message could be solved when the machine and the Schluessel anleitung)

key instruction(?) were known. The analytic answer was: yes; intentionally I do not say the theoretical answer since a correct theory entails a correct practice, otherwise there is an error in theory or practice. So the answer was that a single message could be read given the proper machine: wheel position and all other settings may be unknown, it is only essential to have the machine with the wheels actually used in enciphering. However, what was done in a simplified experiment would in reality have called for a lot of people or a tremendous number of machines (cryptologic aids) so that once again one need hardly count on practical results under normal circumstances.

Not having been concerned with these matters for a long time Fenner can only give certain guiding principles. Assuming he had the machine used and messages enciphered with it, he would assume, let us say, the word "regiment". This plaintext word would be tried with every successive group of eight letters, resetting the machine until at the proper place in the message "regiment" was obtained, with intelligible text before and after the word. Obviously this would call for much time and effort and afterwards would have to be repeated with any change of wheel position or plugging. Chi though that in modern warfare no one would be patient with such loss of time in decipherment and so felt that, correctly used, the Enigma was secure enough.

Another, cleverer method started with the fact that E is the most frequent letter. If two messages are superimposed which are in the same key, then two like letters will appear as like letters and a considerable parts of the coincidences will represent E. From this weak point one went ahead on the assumption that N most often follows E in German. Again the machine was reset again and again until the majority of these assumptions had been proven correct. But here again the time and energy used was so great that they stood in no rational relation to expected results, assuming, of course, that current reading would not be assured by either method. Fenner can no longer give details of this clever attack, it was too complicated to describe with assurance without refreshing his memory by tial with the machine. He made the initial trials, then others took over who could devote themselves to such problems, wherefore he can not now recall details clearly.

9) The only disadvantage of the small Hagelin, say the B 211, is that it produces the cipher text too slowly for present day needs. It has the advantage over the Enigma of being smaller ans still having a far greater period (some 3000000 steps?). Whereas with the Enigma the progress of the period, despite the Rasten (rests or skips?) is relative constant for short stretches, the pinwheels of the Hagelin cause an uneven progress of the period if one conceives the individual steps as function of the normal period. By the riders, expecially when they are easily shifted, a further handy variation is introduced into the rigid system which is stronger (better?) than in the Enigma. So despite certain theoretical equalities and structural affinities the Hagelin represents a material improvement as a substitution system over the Enigma. Hagelin is more modern device, developed and built after the experience with the Enigma was at hand; Enigma deserves recognition as the first cipher machine in practical use which met modern demands for security. It is characteristic of both that when wrongly used they yield messages which in quantity are capable of solution, however, that is no organic fault but merely an evil which can be avoided by proper use. Hagelin's machine does not have reciprocal alphabets. (iii 18-25)

7. M. ary Intelligence Code.

Naturally Chi OKW was interested in USA secret messages : . solution was not achieved. Encipherment appeared complicated with frequent changes, messages close in time showed no parallel passages (repetitions of letter groups)., It was assumed that tables were used and changed daily. ork was discontinued. .

One day the courier from Rome brought a US code. Attempts to use it met with no success. Some months later a courier from Budapest brought some tables, obviously American. These bore a serial number, an indicator, and dates for use. Within an hour messages for the period of the tables was found and success in reading was established. From then on (1941 ?) traffic was read currently even when no tables were available. Sterotype beginnings, phrases, &c were used to break in. Fenner thinks the Mil. Att. at Cairo used the same system. The cipher material he got was photographed. He was told it had been lifted from the baggage of the US ambassador when he was leaving Bucarest (?) or Budapest (?) and was detained for a time in Hungarian territory. His unsealed baggage was opened and the cipher material photographed, the originals were returned promptly and without being noticed. This is the tale told Fenner but he does not know whether it is true. If this system and not that used in Cairo was continued in use till the battles of Tobruk but then replaced, that might have been due to introduction of a machine. Or perhaps the War Dept. had heard that this system had been compromised.

Hellmut Schulz might know more, he was in Weihenkirchen near Bad Aibling in June 1945. (iii 26-27)

8. Fenner's opionion of 15 associates (iii 27-39)

9. Training. In the early 20s there was no uniform vocalulary. The few papers written did detail solution of particular systems but gave no help to one facing an unknown system, no systematic discussion of systems had been attempted. Older men opposed attempts to unify terminology. Fenner set up some problems which departed but little from familiar forms and stumped even the best men. This proved the need of something more than the old trial and error procedure. Some further problems with simple recipherments awakened interest. In informal lectures to small groups he set forth the general characteristics of various types of ciphers and the methods of solving known types which called for only one operation. In the then monthly reports he corrected tirelessly the terms employed and achieved a considerable degree of clarity and logic. He asked that things be expressed so that "even your superior can understand". There were reactions but he regarded them as signs that things were moving. He did forbid others to instruct new comers reserving to himself the training of replacements. In a few years his views had become generally accepted. Decoders, who worked for months or years on the same code came to know it but also got into a rut, when the code was replaced they were lost even though the new code was merely a reshuffling of the same terms so about the mid 20s he gave the elder decoders a course of some 90 days on general principles, basic systems and their combination, and usual encipherments. He always started from a general matter to break the tendency to regard each case as something special. Then special cases were given in the examples and asked criticisms hoping to bring out any systematic features of the system so they could be used cleverly; the students learned to recognize such features and pick out the point of least resistance. Fenner tried to raise cryptology to the status of a science, however, this meant avoidance of any "sure fire" methods, of anything like a Cookbook of Cryptology. He tried to teach the

the methods and leave their application to the judgment, but not the whim, of the student. He also sought on the side to inculcate a certain routine but the main effort was to encourage independent thinking and decision. Hence the program ran:

Meaning of the instruction: Scientific investigation.
Purpose: Training of analysts.
Dissemination of results of previous research.
Collection of new fruits of research.
Comparison of old and new results (criticism).
Arrangement according to certain points of view (Rules, statistics).
Aids, sequence of steps, statistical methods.
Picking out regularities (scientific recognition).

It is evident that the pupils learned also the specific aids such as letter frequencies of foreign languages, bigram and syllable frequencies and their characteristic relations to one another. He also tried to insert mathematics where numbers could serve as measures and the basic rules of Combination (Kombinatorik) and Probability had to be mastered. Although not comprehensive, the results of the course were unmistakable: frequency counts became more acute for discovering possible systematic phenomina, imagination was stimulated, and the notion of Black Art vanished.

As the personnel increased with the years and other duties took more and more time Fenner decided to change the type of instruction. He grouped the more talented younger workers in a course for "General Cryptology" and gave them instructions two days a week from 1500 to 1700 o'clock. The first winter semester on substitutions and in the second winter sememster on transpositions and simple combined systems, also the comonest encipherments. He retained the essentials of his former course but introduced psychological and logical principles since most of the new men had had university educations, and responded to anything that suggested an effort to prove cryptology related to other sciences, i.e. a science itself. He stuck to simple, unadorned presentation of the subject, using examples, historical observations, hints and criticism. New material was incorporated and after two years the pupils were familiar with modern cryptology. He sought to eliminate the unfit and not burden a man capable only of decoding or clerical work with unnecessary ballast. No beginners were admitted. Each expert was to initiate a beginner into the statistics of a plain code, then decipher in a solved code, then assist in work on a partially solved code, and only then attempt a solution by himself. There were exceptions. No applicant was accepted without examination: sample of handwriting, question as to his favorite subjects in school, question in the fields he claimed to know least--not to disconcert him but to judge by his reactions how he would make out in difficult situations. I asked his views on matters which claimed public interest, asked his religious views, tested his Vorstellungsbate (here perhaps comprehension??) and at the end let him talk about his favorite subject so that I could get an idea of his vocabulary and temperament. The candidate had to translate an editorial orally from some foreign paper and make a written translation into the foreign language he claimed to know best. If convinced that the applicant had suitable personality and knowledge he was recommended. T is type of selection and initial training worked out well and was only given up during the war when such personnel had to be accepted as the Arbeitsamt saw fit to provide. Then the teaching became too great a burden "endland and Huettenahin helped Fenner. During the war Huettenhain was assigned to give lectures

TOP SECRET

on advanced cryptology to the more promising workers, this included theory of groups, solution of complex encipherments.codes, the problem of modern machines, i.e. all the things that experience had shown would go beyond the ability of a practical analyst. The idea was due to the assignment during the war of capable young men who expected to return later to their normal careers. Fenner wanted to keep the cryptologic ideas of these men for Chi; reports and long essays would have prevented concentration of the energies of these analysts, mostly university mathemeticians. Hence the method of a talk with discussion, somewhat after the pattern of the seminar, seemed best suited. Thus a distinction came to be made between "lower" and "higher" cryptology, Fenner thinks the courses on both levels were profitable. The bombings and consequent lack of space caused course to be discontinued in Nov. 43.

Huettenhain continued his lectures in the winter of 1944 and 1945 till conditions made this impossible.

The themes of all instruction may be summed up thus:
"A cryptogram is a regular departure from the form of expression in normal writing; recognition of this rule is breaking into the system; mastery of this rule is the solution of the system." This gives the entire problem of the concept "cryptogram" and also the task confronting the cryptanalist. It is the world of his hypotheses and their collapse, of his hopes and disappointments, of his probabilities and his bungling, but also of his certainties and his art. For despite all he may actually learn, there remains in every true cryptanalyist the imponderable of his accomplishment the "spark divine".

It must be accepted as a fact, however strange it may seem to other peoples, that personal security affects the psychological attitude of the German to no unimporant degree. This is not the place to discuss the reasons. But the idea of serving the state all one's life is indissolubly associated with the idea that the state recognized the duty to care for its servants when they are old and unable to work. The state has not avoided this responsibility but has accepted a court decision that one's pension is merely a part of the contratual pay. If this is the norm, than it is not strange if the employee as servant of the state wishes to assure himself of the return service of the state in the form of provision for his old age. In the cipher bureau the analist was "Angestellter" and this category had no pension rights. However he was in constant contact with officers and officials (Beamten) who were entitled to pensions simply because they were in old, established categories. This was felt as an unjust hardship. Some of the older men asked the chief back in the 20s to ascertain the conditions under which an Angesteelter could become a Beamter. There was another reason for this request: these men saw that officers and beamte found doors open in economic life since their activity was not limited to a specialty nowhere else in demand. In the cipher bureau the men feared that due to their limited field they would be in a bad position if dismissed. The fear was not without foundation; Metternich himself had written the Emperor calling attention to the lot of cipher clerks and saying that these men were in their way the most silent and faithful servants of the state who, after a life poor in external honors, must suffer need unless pensioned because their occupation had rendered them inept for finding a suitable place in their old age. However, the initial inquiry by Chi brought no results. In 1927 Fenner was made Beamter to tie him to his job (the military head changed every 3 or 4 ~~years~~, just as he began to know what it was all about). Nothing more happened for years till the Forschungsamt was founded and many of those who deserted Chi to join FA were given Beamten status, this finally aroused higher officials in the Reichswehr ministerium and Fenner was able to get higher rating for several older men. But this,

though welcome, was not a solution of the problem. Competent new men were being added but no prospect of advancement could be held out. The Foreign Office cipher bureau was in a like fix, only the head was Beamter. The difference in standing affected outside relations including efforts to make contracts with business firms, FA men got preference due to rank. Fenner considered that any solution would have to cover the Foreign Office and even the Forschungamt itself. Various organizations had to be heard (Army, Foreign Office, Ministry of the Interior, Ministry of Finace and possibly the Forschungsamt, although this last paid little attention to state regulations). Over a year passed before new career regulations were finally approved and after a 20 year fight some firm ground had been won. The most important points were:

1. Creation of the Beamten (officials) of the upper "foreign language service of the Armed Forces".

2. Applicants. Basically only men with the doctorate or who had passed the "First major State Examination" were admitted. These included: philologists, jurists, mathematicians and natural scientists with full command of one foreign language and some acquaintance with another, Mathematicians needed only one foreign language. As normal requirement came good civic reputation, and for those going to the Armed Forces physical fitness and evidence of having served their prescribed period. Candidates had to pass an examination to prove linguistic or mathematical ability. If passed, the candidate became a "planmässiger" or "Überplanmässiger Regierungsassessor" (according to whether there was an opening or not) with probationary appointment. (The type of examination corresponded to that outlined earlier).

3. Training. Assignment of duties was the same as for any beginner save that the section head who had such an Assessor was required to turn in a report on his progress every 3 months. The candidate had to keep a record of his activities and show it each month. He must also take and show proficiency in the "lower course" in cryptology (2 years). At the earliest the candidate might apply after 3 years for admission to the second grand examination for life Beamter of the Higher Foreign Language Service of the Armed Forces. Admission to examination required of the section head and the chief analist (In the preparation was included lectures on laws governing officials, organization of the Armed Forces, Patent law and Disciplinary law).

4. Examination. First day: translation of some 20 lines of cryptographic or cryptologic text from a foreign language into German; testing some simple cryptographic system which had been offered, e.g. a linear slide or disc or some similar device. Solution of some basic systems with analysis and criticism. (mathematicians took instead some problem from cryptologic mathematics). Total time 6 hours.

Second day: A out 20 minutes text in law, then on cryptography and cryptology for 50 minutes. Not more than 3 candidates at a time.

5. Examination Commission. Head of the Cipher Bureau, chief analist, one of the teachers involved and a representative of the Armed Forces Administrative Office.

6. Results. The comission rated in 9 grades from "deficient" to "praiseworthy". Since the candidated intened to become an administrative official in the legal branches, one point extra credit was given on the legal portion of the examination, before averaging. In case of ties, that candidate was given preference whose bearing during the examination appeared better or whose character was rated higher.

7. If a candidate failed, he was allowed to try again after one year.

No third examination was permitted.

8. Candidates who passed the examination were appointed as Regierungsräten (government counsellors) with all rights and privileges, including the legal right to old age pensions and provision for widow. AS officials of Armed Forces were permitted to wear the uniform of that branch of the Armed Forces they chose and took the appropriate oath.

Since one had no experience to tell whether the requirement could actually be met in the time allowed, provisions was made that changes should be effected by agreement between the examining commissions and the office concerned, e.g. omissions of certain legal questions, extension of time for the cryptanalytic problem. There was no desire to make this a deadly formal test quite out of accord with realities. It was also agreed that only such Beamte should wear uniform as had served their required term lest the public criticize adversly, since only an expert could tell the Beamten uniform from the regular officer uniform.

Fenner believes the new rules were of value. At last anyone could know who could and who could not become an official. Wild claims about "pull" were eliminated and those promoted had the inner satisfaction of knowing they had won the promotion by merit.

The examination was no pro forma matter, it called for proof of real knowledge and ability to take hold. Both examiner and examinee were expected to concentrate. Weeks of hard preparation went into the examinations since, despite the constant changes, they had to be kept equal in difficulty. Conscientious observance of all regulations and adherence to established channels called for real knowledge of the subject and the real responsibility lay on the shoulders of the chief cryptanalist, which in view of the importance of the examinations was a matter of course. (iii 40-53)

#10. VNs. All telegrams were sorted in the telegram registry (logging section ?) by country and brought as quickly as possible to the head of the appropriate section or his representative. There the material was divided according to four points of niew: messages which could be read currently; messages worked on but not presently decipherable; unknown systems, i.e. those not yet analyzed; and extraneous matter, insofar as the logging section had failed to eliminate these.

Those currently dead were stripped of encipherment and/or decoded at once, messages not yet ripe for VNs were tuned over to the expert. Unknown systems were put in collections and, as Chi said, "observed", i.e. watched for like types, frequency of message sending and all criteria which one would like to have cleared up before starting a systematic study. As already stated, good philolicalworkers decoded, naturally new values were always being recovered in the process. Fenner does not hink any clever decoder was allowed to work on more than two plain codes unless breaking had reached a point where only decoding was involved. When messages were decoded the selection began.

Selection. The practiced decoder sees wuickly whether a message contains political of military-political news, is purely administrative, or is without importance. So called Passport messages are quickly spotted, likewise those reporting the Press. Few of these can have objective interest. Moreover nothing is so apt to reduce the value of VNs in the eyes of those who do not know how difficult it is to obtain them, as the publication of every trivial item. Hence in selecting the VNs it was considered important to give: daily situation reports of diplomatic representatives because from them can be gleaned the specific attitude of foreign countries. toward certain problems and finally actually new reports and instructions from the cental authorities to its ambassadors, ministers and plenipotentiaries (and from these to the home office). After observations covering many years about 7 times as many

TOP SECRET

were deciphered as were issued as VNs! Of course instructions were received occasionally regarding information to which special interest was focused but such instructions regularly coincided with what Fenner and his workers knew of current events. He gave his workers as free a hand a s possible in their choice. This was possible since any one concerned with decryption is naturally eager to giveas objectively interestin items as possible even though he may quietly enjoy accounts of a "souper" at which certain gentle n did not handle their knife and fork exactly "comme il faut." The many passport messages and economic messages did not interest the higher-ups and if they were included sometimes, as were even less significant items, it was usually because the decoder from his personal information attributed to them more significance than the (less informed) persons for whom they were prepared. The question: "hat is really important? was, of course, never correctly answered, and can never be fully answered; what seems unimportant today may be intensly interesting 2 years hence. Hence Fenner and his workers took the point of niew that it was better to issue some few unimportant messages than to fail to include some important ones. "Let the higher-ups sift the grain from the chaff."

With straigh army radiograms there was naturally no hard fast criterium for evaluation.. A seemingly irrelevant message in which some new unit was named might, under certain circumstances, be more important than an order to attack, of which one already had knowledge, from other sources. For this reason deciphered army radiograms were never included in the daily VNs, they were termed VNs no doubt but went into different hands where each item was given the necessary careful atention. This work was a separate field, with interpretation of call-signs, the attempt to find some periodicity in the schedule of call signs and wave lengths; with preliminary evaluation, the various card files, the actual evaluation of the message and the final evaluation resulting in an appropriate report, which however has nothing to do with the appropriate and necessary utilization of the secrets. (not clear)

Translation. Very great importance attached to good translation. Translation was necessary since, with the number of languages involved, it as inconceivable that the officers engaged in dealing with theseamessages would be able to understand them all, especially since the grammar in messages often departs from normal usage. In each subsection there was at least one translator analyst who knew the foreign language and German well enough to that in doubtful cases the translation could be shown him for checking. It was expected that such differences as the following be handled correctly:

gewisslich	certainement
sicherlich	surement
nur	plus de, seulement
bloss	pas autrement, simple
anscheinend	probable
scheinbar	apparent

also designations of offices and officials. "hatever might be wrong had to be marked as doubtful, originally by setting (?) after the word, later by dots beneath the enexact passage. However, in view of the multitude of newly appearing technical terms (Fachausdrücke) one or another may not have been rightly rendered. The deciding factor was always the sense of the VN, any attempt at free elaboration of an incomplete report was therefore strictly taboo. For the same reason it was forbidden to introduce personal remarks into the text of a VN; the VN was to come as near as possible to the objective original, else it would have ceased to be a Verlässliche Nachricht. So if an item seemed important enough to be issued as a VN and if it was translated in-

-TOP SECRET-

so German, it was written as a VN.
Distribution. Each VN bore in the heading the designation Chi and VN, also an indication whether send by radio or cable. Then a note of nationality since language alone was not enough. Egypt for instance employed a French code. Furthermore each VN had to contain data which made it a bona fide document; Date of message, and if present, the Journal number (issuing office serial ??). Otherwise in case of publication of historical commentary or sources the opponent might assert that the VN was not genuine! Finally each VN had in the lower left corner a Distribution mark, e.g. "Abw. 4 x." That meant that a total of four copies had been supplied the Abwehr. This mark remained long after Chi ceased to be a part of Abwehr and other offices were supplied copies. No exact list of recipients was on the sheet, for obvious reasons, so it was decided to write "Abw ... x". Hence only the number is correct here this is always to be read "plus 1" since each subsection also had its own complete file of the VN s it produced so that at any time it could look up solved messages or code groups already observed. However, these copies could not appear in the record since otherwise they would have been classified "Kommandosache" and required registration and the office machinery would have become even more complicated. In the lower right corner, also on the last sheet, was a brief indication of the system; e.g. F 21 or Am 1 or Rum 3 &c. This means: France, system No. 21, i.e. the 21st system solved by Chi since World War I; the first American system so solved or the 3rd Romanian system. This notation was sometimes made more explicit, i.e. the intire formula for the system was given, e.g. P4ZC8Zw4 meaning: Polish 4 digit code enciphered by additive sequence (Zahlenwurm), fourth system solved. Later these notations were usually made only on the copy which remained in the section, hence a VN may be genuine without such mark; its significance was only for the secton anyway. On many VNs there may appear also the cipher (initials) of the respônsible worker and my own, the latter dripped out later since it was impossible to read all VNs. VNs were reproduced on the typewriter (with carbons), the carbon paper got worse and worse and led to complaints but not till 1944 could Fenner get permission to use "Wachsplatten" (some multigraph?) and pull the required number of copies. As soon as the copies were made they were taken without loss of time to Lt. Kalckstein who was charged with all further details. He kept the one copy which ultimately went to the Archive. These copies were inserted in Laitzordner (binders?) annually, later monthly, and delivered to the Chef der Heeresarchive, Potsdam, Hans von Seeckt Strasse 8, whenever it was assumed that Chi had no longer an active interest in them. All VNs up to about 1930 were delivered there, the remaining material that was ready for the Archive was in the main bulding in the Tirpitzufer or in Fenner's office, where the sets for several years were burned. The Ordner (binders) were assigned serial numbers, the genuineness of such documents could be proven at any time.

Fenner know nothing about the distribution keys (lists) and did not bother with the subject, this was Kalckstein's affair along with control of copies returned. As he recalls, some 10 copies were made at the last and the matrices burned in Fenner's office. Before distribution the most important passages in the messages were underscored by Kalckstein and his assistants; opinions as to the value of this varied. Fenner and Schadel objected to this "predigestion" because of the danger that there was danger that the reader would scan these valuable documents just as fleetingly as he did others. They maintained that VNs should only reach the hands of those who had time to look at each one until he understood it. Those who would read VNs for sensational items ought not to see them at all. However others were of a different

opinion and underscored certain words with colored pencil. Assuming clever, serious readers this may be very good, but only under the presupposition stated above. After Fenner succeeded in having the VNs multigraphed (dittoed?) the Call sign was added under the heading (for the statistics of other Chi sections) and a brief summary was prefixed. This was necessary because along with the modernization of the reproduction went the organization of the archive and the card file. He also hoped the abstracts would do away with the underscoring and also force decripters and translators to give attention to the content.

Publication. Publication of VNs was strictly forbidden. Each VN was classified as Secret. (Geheime Kommandosachs) and enjoyed the highest security protection. It was forbidden to mention VNs and decip erment outside of the office and inside only with those personally known, not with unknown officers and officials, so called visitors who came in on one pretext or another. Every serious cryptologist knows the consequences of publication of a VN. When Ambassador Page published the Zimmermann despatches after World War I Chi used these to prove how important exact decipherment is and how important it is that every cryptographic system be tested before being put into use. And Page's publication was worth more than a whole series of lectures. Once when an English correspondent obtained knowledge in AA of an Italian VN deciphered by Chi and published it in the Manchester paper, including an error in decipherment. This Italian system was replaced and Ambassador Amadori (who, as Fenner recalls, was then in Riga) was likewise replaced. In general the rule was that publication of all sources 25 years after an important event is as soon as it will serve the truth. Earlier may be very intriguing but there will be so many decent people involved, people who have erred not from bad motives but solely from human inadequacy, that it is better to maintain silence and wait. (For this reason there was still no exact story of certain events of World War I). When the French Intelligence Service learned that Chi was working successfully on French diplomatic ciphers, this information alone was enough to induce the Quay d'Orsay to replace certain ciphers sooner than was its want. Thus not only every publication but de facto every rumor, represents a danger for one's cryptologic work, the purpose of which is not lust for sensation but promotion of the security of the country one serves, with means which one prefers to employ when dynamite and aceteline torch would draw too much public attention, and would endanger it without bringing the slightest gain. (iii 53-61)